

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**



AIR FORCE INSTRUCTION 31-113

26 JANUARY 2012

**AIR NATIONAL GUARD
Supplement**

15 MARCH 2013

Security

**INSTALLATION PERIMETER ACCESS
CONTROL**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is only available directly from the OPR.

RELEASABILITY: Access to this publication is restricted. This publication is for official use only (FOUO); requests for accessibility must be approved by the OPR.

OPR: AF/A7SO

Certified by: AF/A7S
(Brig Gen Jimmy E. McMillian)

Pages: 107

(ANG)

OPR: NGB/A7SO

Certified by: NGB/A7S
(Lt Col John D. Conaway)

Pages: 3

This Air Force Instruction (AFI) implements Air Force Policy Directive (AFPD) 31-1, *Integrated Defense*. Compliance with this Instruction is mandatory and applies to all military and civilian Air Force (AF) personnel, members of the Air Force Reserve and Air National Guard, and other individuals or organizations as required by binding agreement or obligation with the Department of the Air Force. In addition, this Instruction is mandatory for all government-owned, contractor-operated (GOCO) and contractor-owned, contractor-operated (COCO) facilities when required by contractual agreement. The terms "must," "shall," and "will" denote mandatory actions in this Instruction. This Instruction requires the collection and maintenance of information protected by the Privacy Act of 1974. System of Records Notices (SORN) F031 AF SP F, *Notification Letters to Persons Barred from Entry to Air Force Installations*, F031 AF SF B, *Security Forces Management Information System (SFMIS)* and F031 AF SP O, *Documentation for Identification and Entry Authority*, applies. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>. This Instruction amplifies Department

FOR OFFICIAL USE ONLY

of Defense (DoD) security standards and guidance for authorizing physical access to United States Air Force (USAF) installations and/or stand-alone facilities, as required by the following: Section 1069, 2008 *National Defense Authorization Act (NDAA)*; Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*; Under Secretary of Defense, Intelligence [USD(I)] Directive Type Memorandum (DTM) 09-012, *Interim Policy Guidance for DoD Physical Access Control*; DoD 5200.08-R, *Physical Security* and Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. Further, it builds upon the minimum installation access standards as established by the Chief of Staff of the Air Force (CSAF) memorandum dated 3 March 2004 (SUBJ: *Protect the Force: Establishing the New Baseline Force Protection Posture*) and expands and rescinds the USAF Vice Chief of Staff (VCSAF) memorandum dated 8 Sep 09 (SUBJECT: *Air Force Policy for Installation Access Control*); and references Air Force tactics, techniques and procedures (AFTTP) 3-31.1, *Entry Control*. All Security Forces (SF) units are required to maintain a printed copy of AFI 31-113 in case of emergencies as well as for informational and training purposes. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field through the appropriate functional chain of command. Contact supporting records managers as required. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the AF. Affected organizations have 180 days from date of publication to implement this AFI or submit applicable deviations to the appropriate deviation authority. Major Commands, Direct Reporting Units (DRUs) and Field Operating Agencies (FOAs) will send one copy of supplements to Headquarters, Air Force Security Forces Center (HQ AFSFC), Police Services (SFOP), 1517 Billy Mitchell Boulevard, Lackland Air Force Base (AFB) TX 78236.

(ANG) This supplement modifies Air Force (AF) policies and procedures found in Air Force Instruction, (AFI) 31-113, *Installation Perimeter Access Control*. It identifies specific responsibilities for implementing access control in the Air National Guard (ANG). Local instructions, policies, procedures and the like that are not consistent with this instruction should be evaluated for revision.

(ANG) Compliance with this instruction is mandatory and applies to all Air National Guard (ANG) military and civilian personnel including contract personnel responsible for its implementation.

(ANG) Records disposition. Ensure that all records created by this AFI are maintained and disposed of IAW AFRIMS.

Chapter 1—CONCEPT, PLANNING, AND RESPONSIBILITIES	7
1.1. Objective.	7
1.2. Overarching Guidance.	8
1.3. Authority.	9

FOR OFFICIAL USE ONLY

1.4.	The protection of civil liberties, privacy and Personally Identifiable Information (PII).	9
1.5.	Responsibilities.	9
Chapter 2—INSTALLATION PERIMETER ACCESS CREDENTIALS		18
2.1.	Source Documentation.	18
2.2.	Common Access Cards (CAC).	18
Figure 2.1.	Armed Forces of the United States Geneva Conventions Card.	21
Figure 2.2.	U.S. DoD and/or Uniformed Services ID Card.	22
Figure 2.3.	U.S. DoD and/or Uniformed Services ID and Privilege Card.	23
Figure 2.4.	U.S. DoD and/or Uniformed Service Geneva Conventions ID Card for Civilians Accompanying the Armed Forces.	25
2.3.	Non-Common Access Card (CAC) Department of Defense (DoD) Credentials. ..	25
Figure 2.5.	DD Form 2, United States Uniformed Services Identification Card (Retired).	27
Figure 2.6.	DD Form 2, Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green).	28
Figure 2.7.	DD Form 2, United States Uniformed Services Identification Card (Reserve Retired).	29
Figure 2.8.	DD Form 1173, Uniformed Services Identification and Privilege Card.	30
Figure 2.9.	DD Form 1173-1, Department of Defense Guard and Reserve Dependent Identification Card.	31
Figure 2.10.	DD Form 1934, Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces.	33
Figure 2.11.	DD Form 2764, United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card.	34
Figure 2.12.	DD Form 2765, Department of Defense/Uniformed Services Identification and Privilege Card.	34
Figure 2.13.	Civilian Retiree Card.	36
2.4.	Non-Department of Defense (DoD) Federal Personal Identity Verification (PIV).	36
Figure 2.14.	DHS Federal PIV.	37
2.5.	Transportation Worker Identification Credential (TWIC).	37
Figure 2.15.	TWIC.	38
2.6.	Personal Identity Verification-Interoperable (PIV-I).	38
2.7.	Locally Produced Physical Access Control System (PACS) Passes/Cards and AF Form 75 Visitor Pass/Vehicle Pass.	38

Figure 2.16.	DBIDS Card.	40
2.8.	Approved Department of Defense (DoD) Privilege Card Holders.	40
2.9.	Veterans Identification Card (VIC).	41
Figure 2.17.	Veterans Identification Card.	41
2.10.	Privatized Housing.	42
2.11.	Air Force Office of Special Investigation (AFOSI) Special Agents.	42
2.12.	Federal Bureau of Investigation (FBI) and United States Secret Service (USSS) Special Agents.	42
Chapter 3—IDENTITY PROOFING AND REGISTRATION		43
3.1.	Identity Proofing Concept.	43
3.2.	Common Access Card (CAC) Populations.	43
3.3.	Non-Common Access Card (CAC) Department of Defense (DoD) Populations. .	43
3.4.	Non-Department of Defense (DoD) Federal Personal Identity Verification (PIV) Populations.	43
3.5.	Transportation Worker Identification Credential (TWIC) Holders.	43
3.6.	Personal Identity Verification-Interoperable (PIV-I) Credentials.	43
3.7.	Locally Produced Physical Access Control System (PACS) Passes/Cards and AF Form 75 Visitor Pass/Vehicle Pass.	43
Figure 3.1.	United States Passport.	46
Figure 3.2.	Permanent Resident Card/Alien Registration Receipt Card (Form I-551).	47
Figure 3.3.	Foreign passport with a temporary (I-551) stamp or temporary (I-551) printed notation on a machine readable immigrant visa.	48
Figure 3.4.	An employment authorization document that contains a photograph (Form I-766).	49
Figure 3.5.	Current/Valid Driver's License.	50
Figure 3.6.	Identification card issued by Federal, State or local Government Agencies.	51
Figure 3.7.	U.S. Coast Guard Merchant Mariner Legacy Cards.	52
Figure 3.8.	U.S. Coast Guard New Merchant Mariner Credential.	53
3.8.	Approved Department of Defense (DoD) Privilege Card Holders.	55
3.9.	Veterans Identification Card (VIC).	55
3.10.	Outside the Continental United States (OCONUS).	56
3.11.	Registration.	56
3.12.	Unique Considerations/Special Events/Exceptions to Policy.	57
Chapter 4—IDENTITY VETTING AND FITNESS DETERMINATION		58

4.1.	Identity Vetting Concept.	58
4.2.	Common Access Card (CAC) Populations.	58
4.3.	Non-Common Access Card (CAC) Department of Defense (DoD) Populations. .	58
4.4.	Non-Department of Defense (DoD) Federal Personal Identity Verification (PIV) Populations.	58
4.5.	Transportation Worker Identification Credential (TWIC) Holders.	58
4.6.	Personal Identity Verification-Interoperable (PIV-I) Credentials.	58
4.7.	Locally Produced Physical Access Control System (PACS) Passes/Cards and AF Form 75 Visitor Pass/Vehicle Pass.	59
4.8.	Approved DoD Privilege Card Holders.	60
4.9.	Veterans Identification Card (VIC).	60
4.10.	Foreign Visitors.	60
4.11.	Housing Privatization Personnel.	60
4.12.	Non-authoritative Databases.	61
4.13.	Fitness Determination.	61
4.14.	Debarment.	63
Chapter 5—	PERIODIC SCREENING REQUIREMENTS OVERVIEW	67
5.1.	Inherent Vulnerability.	67
5.2.	Procedures.	67
Chapter 6—	INSTALLATION PERIMETER ENTRY CONTROL POINT OPERATIONS	69
6.1.	United States Air Force (USAF) Installation Perimeter Access Control Guidance.	69
6.2.	Construction Standards.	69
6.3.	Installation Perimeter Access Control Measures.	70
6.4.	Installation Perimeter Access Control Minimum Standards for Controlling Physical Access.	73
6.5.	Escort Authority.	75
6.6.	Sponsorship.	76
6.7.	Installation Perimeter Access Control Procedures for Emergency Responders and Civilian Law Enforcement.	77
6.8.	Internal Access (to include Service-determined controlled, restricted, and limited areas).	77
6.9.	Identification/Verification.	77
Chapter 7—	IDENTITY MANAGEMENT ENTERPRISE SERVICES ARCHITECTURE	79

7.1.	Source Documents.	79
7.2.	Identity Management Enterprise Services Architecture Requirements.	79
7.3.	Continuous Information Management Capability.	80
Chapter 8—BIOMETRICS		81
8.1.	Overview.	81
8.2.	Requirements.	81
8.3.	Biometric Categories.	82
8.4.	Biometric Standards.	83
8.5.	Local Guidance Requirements.	83
Chapter 9—TRAINING AND EXERCISES		84
9.1.	Concept.	84
9.2.	Training.	84
9.3.	Exercises.	84
9.4.	Lessons Learned, Vulnerabilities, and Higher Headquarters Feedback.	85
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		86

Chapter 1

CONCEPT, PLANNING, AND RESPONSIBILITIES

1.1. Objective. The objective of installation perimeter access control is to restrict and/or control entrance to property and/or installations to only those authorized persons and their vehicles to protect personnel, resources and missions.

1.1.1. Installation perimeter access control procedures include identity proofing, vetting to determine the fitness of an individual requesting and/or requiring access to installations, and issuance of access credentials.

1.1.1.1. Identity proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) when attempting to establish an identity.

1.1.1.2. Vetting: An evaluation of an applicant's or a card holder's character and conduct for approval, acceptance or denial for the issuance of an access control credential for physical access.

1.1.1.3. Fitness: Level of character and conduct determined necessary for the basis of access control decisions. For the purposes of this instruction, fitness is further defined as follows:

1.1.1.3.1. Person presenting the credential has been properly identity proofed and vetted. **Note:** Dependents are currently exempt from vetting, and the authorized card holder sponsoring them assumes the risk.

1.1.1.3.2. Person has a credential authorized to facilitate access.

1.1.1.3.3. Person matches the credential authorized to facilitate access.

1.1.1.3.4. Person with credential authorized to facilitate access is authorized access to that particular installation. **Note:** Possession of a valid/authorized credential does not automatically authorize access to that installation. The individual must still have a valid purpose to be on the installation and properly sponsored, as applicable.

1.1.1.3.5. Authorized credential is still valid and not expired.

1.1.1.3.6. Person with credential authorized to facilitate access is still fit since last vetting as determined via continuous information management. **Note:** This continuous information management will be accomplished via the Identity Management Enterprise Services Architecture detailed in Chapter 7.

1.1.1.3.6.1. Person is not on a terrorist watch list.

1.1.1.3.6.2. Person is not on the installation's debarment list.

1.1.1.3.6.3. Person is not on a felony wants and warrants list.

1.1.2. Persons authorized access shall be either escorted or unescorted:

1.1.2.1. **Escorted Individuals**—Personnel who require access, without determination of fitness, who must be accompanied by a sponsor with authorization to escort the

FOR OFFICIAL USE ONLY

individual. The escort requirement is mandated for the duration of the individual's visitation period.

1.1.2.2. **Unescorted Individuals**—Personnel who have been identity proofed and favorably vetted are eligible for unescorted access within the installation; but are still subject to any controlled or restricted area limitations, as appropriate.

1.1.3. Commanders or directors will employ access control measures at an installation perimeter to enhance security and protect personnel, resources and installations.

1.1.4. Successful installation access control is:

1.1.4.1. Pivotal to integrated defense (ID) and force protection (FP) because it improves the probability of detection and provides a strong psychological deterrent to those who may pose a threat to installation resources and personnel.

1.1.4.2. Accomplished by establishing a physical boundary around installations, channeling personnel and vehicles to designated entry control points (ECPs) for processing, developing a standard to determine who is authorized physical access, and maximizing the ability to detect those individuals attempting to subvert established procedures and gain unauthorized access to the installation.

1.2. Overarching Guidance.

1.2.1. The standards prescribed herein are the minimum required for United States Air Force (USAF) installations and must be adhered to. Combatant Commanders (COCOM), Major Command (MAJCOM) Commanders and Installation Commanders may authorize additional security requirements based upon the type of installation, mission, enemy, terrain and weather, troops and support available-time available and civil considerations (METT-TC), resources, category of individuals requiring access, Force Protection Conditions (FPCONS), a completed Integrated Defense Risk Management Process (IDRMP), level of access to be granted and other emerging contingencies, as necessary.

1.2.1. (ANG) Deviations to this instruction will adhere to and follow the process of the Deviation Program as outlined in AFI 31-101, *Integrated Defense*.

1.2.2. USAF installations will meet applicable physical security standards for installation perimeters in accordance with (IAW) Air Force Instruction (AFI) 31-101, *Integrated Defense*.

1.2.3. New and modified facilities will comply with either Unified Facilities Criteria (UFC) 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*, or with a properly approved waiver or exemption.

1.2.4. For OCONUS locations, MAJCOMs and Installation Commanders may deviate from the requirements where local conditions, treaties, agreements, foreign governments and allied forces require different standards. Commanders will work with local and foreign authorities to identity proof and vet applicants to the greatest extent practical and lawful.

1.2.5. This AFI does not negate other USAF protection and security requirements governed by instructions and manuals implementing and guiding force protection, physical security, nuclear security, and antiterrorism (AT).

FOR OFFICIAL USE ONLY

1.2.6. To ensure effective use of resources, long-term sustainability and joint interoperability, installations will coordinate all installation and internal access control systems and components with MAJCOM A7S Divisions and the AFSFC/SFXR (Requirements Branch) prior to funding obligation and execution.

1.2.6. (ANG) ANG units will identify installation and internal access control systems and components via the Security System Project Description (SSPD) process.

1.2.7. Any systems which connect to the USAF Global Information Grid (GIG) must be accredited and certified in concert with local and USAF communications entities and a thorough Privacy Impact Assessment (PIA) accomplished IAW AFI 33-332, *Air Force Privacy Program*. **Note:** For clarification, a PIA is required for systems that collect personally identifiable information (PII). This process is completed on a DD Form 2930, *Privacy Impact Assessment*, and sent to the Air Force Privacy Officer to be staffed for approval.

1.2.8. Installation Commanders will coordinate and seek to standardize and integrate access control procedures and local credentials with other military installations in the local area as defined in all regionally located Services' directives.

1.3. Authority. Authority to control access to USAF installations varies based on jurisdiction, property rights, and geographic location.

1.3.1. Continental United States (CONUS), Alaska, Hawaii and US Territories and Possessions. Within United States (US) jurisdiction, commanders publish and enforce guidance to protect installation resources IAW DoD and USAF policy. In addition, Department of Defense Instruction (DoDI) 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, prohibits individuals from entering military installations within the jurisdiction of the United States for a purpose prohibited by law or lawful regulation or reentering an installation after being ordered not to reenter by any officer in command of the installation.

1.3.2. Outside the Continental United States (OCONUS). Outside the United States, a commander's right to exercise this authority comes from United States laws and Status of Forces Agreements (SOFAs) applying in the overseas area and from bilateral and multilateral agreements between the United States and the host nation.

1.3.2.1. Expeditionary Locations. In addition to OCONUS jurisdiction as indicated in paragraph 1.3.2., jurisdiction, rules of engagement (ROE) and legal authority may also be determined by laws of war and supplemental general orders (GO).

1.3.2.2. Commanders at all levels are responsible to ensure USAF personnel understand their legal authority, jurisdiction and ROE.

1.4. The protection of civil liberties, privacy and Personally Identifiable Information (PII). PII collected and utilized in the execution of this AFI must be safeguarded to prevent any unauthorized use, disclosure and/or loss. Installations shall ensure that the collection, use and release of PII complies with the requirements of DoD Directive (DoDD), 5400.11, *DoD Privacy Program*, DoD 5400.11-R, *Department of Defense Privacy Program*, DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, and AFI 33-332.

1.5. Responsibilities.

FOR OFFICIAL USE ONLY

1.5.1. Office of Information Dominance and Chief Information Officer (SAF/CIO A6):

1.5.1.1. Serves as the USAF lead agency for biometrics, network integration and the principal Air Force representative to the Biometrics Identity Management Agency (BIMA), the DoD's Executive Agent for Biometrics.

1.5.1.2. In concert with the BIMA and DoD General Counsel, provides oversight to the implementation of biometrics within access control systems in accordance with DoD and USAF policy and directives.

1.5.2. Office of the Legislative Liaison, Foreign Disclosure and Technology Transfer Division (SAF/IAPD): Serves as the USAF proponent for Foreign Visit System (FVS) and FVS-Confirmation Module (FVS-CM).

1.5.3. The Office of the Deputy Chief of Staff for Logistics, Installations and Mission Support, Directorate of Security Forces (AF/A7S):

1.5.3.1. Is the Chief of Staff of the Air Force's (CSAF's) primary advisor for law and order operations and installation access control.

1.5.3.2. Assists Under Secretary of Defense, Intelligence (USD(I)) with the development of DoD access control policy and the minimum DoD security standards for controlling entry to DoD installations and stand-alone facilities.

1.5.3.3. Develops overarching, USAF installation perimeter access control policy and is the approval authority for law and order and access control guidance.

1.5.3.4. Plans, develops and monitors all USAF access control programs.

1.5.3.5. Develops and coordinates USAF law and order policy directives and approves and publishes identification (ID) specific Air Force tactics, techniques and procedures (AFTTPs) and Air Force Manuals (AFMANs).

1.5.3.6. Manages distribution of access control equipment and systems received through central procurement.

1.5.3.7. Manages the access control Program Objective Memorandum (POM) funding process.

1.5.3.8. Serves as functional approval authority for manpower standards related to installation access control.

1.5.4. Air Force Security Forces Center (AFSFC):

1.5.4.1. Drafts and coordinates USAF access control instructions, manuals and tactics, techniques, and procedures (TTPs).

1.5.4.2. Defines Security Forces (SF) capability sets and defines capability standards, applicability and effects of delivery.

1.5.4.3. Develops mission essential task lists (METLs) and associated training tasks, conditions and standards.

1.5.4.4. Coordinates access control guidance with other programs and functional specialties.

1.5.4.5. Incorporates and adapts access control guidance into AFIs; develops installation access control standards and procedures; and monitors the effectiveness of the access control program.

1.5.4.6. Provides expertise in operational guidance development in the areas of law and order operations and military working dog (MWD) employment.

1.5.4.7. Plans, develops and reviews programs concerning access control training.

1.5.4.8. Reviews access control training requirements and recommends curriculum changes.

1.5.4.9. Incorporates findings into the AFSFC Lessons Learned process.

1.5.4.10. Develops SF tactical doctrine and concepts in order to execute the access control mission (home station and deployed bases).

1.5.4.11. Drafts guidance to support new SF initiatives.

1.5.4.12. Reviews AF policy and recommends changes to support development of SF concepts and guidance.

1.5.4.13. Manages the Air Force Vulnerability Assessment (AFVA) programs and conducts AFVAs as required. Evaluates access control policy and procedures during vulnerability assessments.

1.5.5. Logistics, Installations & Mission Support Directorate, Asset Management & Operations Division (AF/A7CA): Provides recommendations and inputs to access control procedures relative to AFI 32-6007, *Privatized Family Housing*.

1.5.6. Air Force Civil Engineer Support Agency (AFCESA):

1.5.6.1. Provides field expertise, recommendations, support and other input for structural, environmental, Fire Emergency Services, Explosive Ordnance Disposal (EOD), Emergency Management (EM), Chemical, Biological, Radiological, Nuclear or High Yield Explosives (CBRNE) operations, and other engineer areas of expertise.

1.5.6.2. Provides recommendations to MAJCOMs in reconciling force protection construction standards with airfield planning and design standards.

1.5.6.3. Ensures engineers have input in acquiring necessary equipment and resources by coordinating their conditions and limitations into Air Force requirements for research and development efforts.

1.5.6.4. Is responsible for the UFC system.

1.5.7. Air Force Office of Special Investigations (AFOSI):

1.5.7.1. Provides counterintelligence (CI) activities to include collection and production of information concerning foreign intelligence, investigations of terrorism, sabotage and related acts, offensive operations against foreign intelligence services and AT services.

1.5.7.2. Provides the Defense Force Commander (DFC) CI information within the area of interest as well as establishing an effective liaison with host nation (HN) intelligence, security, and law enforcement sources.

1.5.7.3. Maintains the capability to respond to criminal activities.

1.5.7.4. Provides immediate, worldwide, complementary support to the deployed area commander by conducting specialized CI support to FP, protective service operations, and counter-threat operations.

1.5.7.5. Plans and programs support to counter-threat operations.

1.5.8. MAJCOM Commanders:

1.5.8.1. Establish assessment and planning staffs as appropriate.

1.5.8.2. Direct development of operational level access control planning as required.

1.5.8.3. Direct validation of manpower and resource allocation in support of access control.

1.5.9. Air National Guard (ANG): Organizes, trains, and equips ANG SF units for wartime duties in coordination with the gaining MAJCOM/A7S and AF/A7S.

1.5.10. Air Force Reserve Command (AFRC): Organizes, trains and equips AFRC SF personnel for garrison and/or expeditionary roles/duties and coordinates with the gaining MAJCOM Security Forces (MAJCOM/A7S) and USAF/A7S as required.

1.5.11. MAJCOM/A7S:

1.5.11.1. Identifies command-wide training requirements.

1.5.11.2. Incorporates access control into SF Phase I and II Training programs as necessary IAW AFI 36-2225, *Security Forces Training and Standardization and Evaluation Programs*.

1.5.11.3. Develops procedures for documenting training results.

1.5.11.4. Prepares plans and documents for acquisition of necessary installation perimeter access control equipment.

1.5.11.5. Makes recommendations to AF/A7S and AFSFC on policies concerning organizing, training and equipping units and forces to provide installation perimeter access control.

1.5.11.6. Develops and submits security requirements in supplements to this instruction, security requirements for MAJCOM-unique systems, resources and facilities.

1.5.11.7. Validates entry control posts during the manpower standard implementation post validation process.

1.5.11.8. Ensures force protection and security construction projects are integrated with MAJCOM Airfield/Community Planner airfield design and protection criteria.

1.5.12. Installation Commanders:

1.5.12.1. Responsible for the defense and protection of the installation.

1.5.12.2. Responsible for chartering the Integrated Defense Council (IDC) to implement programs for the protection of personnel, property, resources and missions under their control. Programs must meet DoD and USAF protection criteria.

1.5.12.3. Establish commander's intent and define risk tolerance in relation to installation perimeter access control.

FOR OFFICIAL USE ONLY

1.5.12.4. Assume, accept, remediate or mitigate risk for assigned assets as appropriate.

1.5.12.5. Elevate risk decisions to higher echelons when appropriate.

1.5.12.6. Appoint the DFC as the installation's OPR to coordinate installation access control IAW this instruction.

1.5.12.7. Establish working groups, staffs, and executive councils to conduct and oversee defense and protection assessments and planning as necessary and as required by instruction.

1.5.12.8. Maintain liaison with adjacent installations, base clusters and supporting HN security agencies, and civil authorities within the joint base boundary as defined in Joint Publication 3-10, *Joint Security Operations in Theater*, or around the Installation Commander's jurisdictional boundaries. See AFI 31-101, AFI 10-245, *Antiterrorism*, and AFTTP 3-10.2, *Integrated Base Defense Command and Control*, for additional information. **Note:** Responsibilities for liaison may be retained by higher authority or delegated to subordinate commands as local circumstances dictate.

1.5.12.9. Where applicable, integrate area security plans with the Joint Security Office and the appropriate operations center that coordinates security in areas where security forces operate.

1.5.12.10. In alignment with DoD, Service, COCOM, combined joint forces command, and MAJCOM policies, identify specific procedures for access credential issuance on the installation. This includes rules associated with sponsorship/need determination, identity proofing, identity vetting/fitness determination, credential issuance (form of temporary credentials as well as the visual authenticators associated with them) or denial, access control operations/screening, periodic re-vetting of identities, and vehicle and container searches, as applicable.

1.5.12.11. Determine local credential requirements for personnel under the age of 18 who require non-recurring access and are not in possession of an authorized identification credential or identity source document listed in Chapter 2.

1.5.12.12. Implement procedures for off base first responders' physical access requirements during emergencies.

1.5.12.13. Delegate personnel to perform identity proofing, vetting and determination of fitness, and access authorizations and privileges.

1.5.12.14. Determine the number of personnel that approved escorts are authorized to escort and sponsorship and escort rules for DoD dependents under the age of 18.

1.5.12.15. Ensures force protection and security construction projects are integrated with MAJCOM Airfield/Community Planner airfield design and protection criteria.

1.5.13. Unit Commanders:

1.5.13.1. Each unit commander, tenant unit commander, or agency chief or equivalent staff agency chief must ensure their personnel understand and follow installation access control guidance and procedures.

1.5.13.2. Each unit commander, tenant unit command, or agency chief or equivalent staff agency chief must identify to the IDC key missions and associated resources required to execute this instruction continuously or with minimal delay even in heightened security situations; and coordinate and integrate all associated IDC processes to enhance mission continuity.

1.5.14. Defense Force Commanders (DFCs):

1.5.14.1. Serves as the Installation Commander's primary advisor for Law and Order operations and installation access control. On USAF installations, the SF squadron commander is the DFC. On USAF installations with more than one SF squadron, the DFC is the SF commander responsible for installation security and Law and Order operations.

1.5.14.1. (ANG) In their absence, the DFC may delegate day-to-day duties and advisory role to the senior security forces member present for duty. However, the DFC will retain all responsibility as the primary advisor for Law and Order operations and installation access control. The acting primary advisor shall coordinate and inform the DFC of all issues/actions taken in the DFC's absence.

1.5.14.2. Maintains command and control (C2) of Law and Order operations. This C2 is executed through the Base Defense Operations Center (BDOC).

1.5.14.3. Exercises operational control (OPCON) over all assigned Law and Order forces.

1.5.14.4. Conducts access control assessments and planning.

1.5.14.5. Develops and publishes the IDP, incorporates law and order and installation access control policies and procedures into the IDP, and develops installation access control standards and procedures.

1.5.14.6. Establishes procedures for DoD ID-card holders to register in and withdraw from the Physical Access Control Systems (PACS) during in and out-processing at the servicing location.

1.5.14.7. Coordinates the inclusion of registration and deregistration into PACS on base/installation in-processing and out-processing checklists. Since PACS are designed to associate each DoD ID with a specific individual, re-registration is required anytime an ID card is reissued for any reason (e.g. loss, confiscation or normal replacement).

1.5.14.8. Establishes procedures for ensuring responsible sections/organizations retrieve PACS credentials and locally created access credentials from individuals who no longer require installation access.

1.5.14.9. Establishes provisions to ensure only users who have been trained to operate the PACS have access to the equipment.

1.5.14.10. Establishes procedures to protect PACS equipment against theft or damage at operating locations and access control points. **Note:** If the facility where the equipment is housed cannot be secured, the equipment must be removed at the end of the duty day.

1.5.14.11. Manages current and future requirements based on operational deficiencies and provides oversight in the development, review and validation of emerging technology to fulfill operational capabilities at the installation level.

1.5.14.12. Participates in installation working groups as required.

1.5.14.13. Works closely with installation AT Officers and Information Protection Offices (IPO) to develop local guidance and concepts to execute the law and order and access control missions.

1.5.14.14. Documents required entry control posts in the post priority chart annex of the IDP.

1.5.14.15. Determines posts that will go unmanned and how available resources will be used during times of funding or personnel shortages.

1.5.14.16. Ensures current debarment information is loaded into the Security Forces Management Information System (SFMIS) and appropriate PACS databases as necessary.

1.5.14.17. Identifies an SF section for the registration and issuance of installation access credentials listed below and ensures section personnel are trained, proficient, and certified in their assigned responsibilities relating to:

1.5.14.17.1. Air Force (AF) Form 75, *Visitor/Vehicle Pass*.

1.5.14.17.2. PACS created passes/cards.

1.5.14.17.3. Access Control Lists, or other measures associated with accounting for access control and who is authorized entry.

1.5.14.18. Establishes procedures to receive reports of lost/stolen ID cards or access credentials IAW paragraph 1.5.17.4.

1.5.15. Force Support Squadron (FSS) Commanders will:

1.5.15.1. Ensure Military Personnel Elements issue CACs to applicable populations IAW Homeland Security Presidential Directive -12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*; Under Secretary of Defense for Personnel and Readiness (USDP&R) Directive Type Memorandum (DTM) 08-003, *Next Generation Common Access Card (CAC) Implementation Guidance*, and AFI 36-3026 (IP), Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*.

1.5.15.2. Ensure procedures for DoD ID-card holders are followed to register and withdraw from PACS during in and out processing.

1.5.15.3. Ensure individuals requiring access are properly vetted prior to issuance, as appropriate.

1.5.15.4. If a local access credential is not returned, the installation commander may consider base debarment, as applicable. If debarment occurs, promptly notify the applicable contracting officer.

1.5.16. Sponsoring Organizations will ensure:

FOR OFFICIAL USE ONLY

1.5.16.1. The appropriate registration form is prepared for each access credential applicant.

1.5.16.2. The applicant registers his or her vehicle according to the procedures established in the Area of Operation (AO).

1.5.16.3. Prospective contractor employees are escorted from the installation entry control point to the appropriate office to initiate identity proofing and vetting for the appropriate credential issuance as determined by the duration of the contract.

1.5.16.4. Include in all purchase requests the requirements for contractor personnel to return all local access credentials to the issuing office when the contract is completed or when a contractor employee no longer requires access to the installation (e.g. quits, contract is terminated, etc.).

1.5.16.5. Include a contract provision to ensure that contractors return all local access credentials to the issuing office when the contract is completed or when a contractor employee no longer requires access to the installation (e.g. quits, contract is terminated).

1.5.16.6. Issued access credentials are retrieved and returned to the issuing office when the relationship that served as justification changes or is terminated.

1.5.16.7. Provide information relevant to the FVS and FVS-CM on CONUS installations.

1.5.16.8. Personnel designated authority to serve as approving officials are identified to the credential issuance office.

1.5.17. All personnel requiring recurring and unescorted access to USAF installations with PACS must:

1.5.17.1. Enroll their credential authorized to facilitate access in the PACS according to locally established guidance.

1.5.17.2. Carry their DoD ID card or approved credential on their person while in duty status or when on a USAF installation.

1.5.17.3. On request, present their DoD ID card or approved access credential to Law and Order or security personnel. Individuals who refuse to present their DoD ID card or approved credential are subject to immediate surrender of the credential and may be subject to further administrative or punitive action.

1.5.17.4. Immediately report a lost or stolen DoD ID card or access credential to the local SF, and issuance office so the card can be deregistered.

1.5.17.4.1. For CACs, the individual shall be required to present documentation from the local security office or CAC sponsor confirming that the CAC has been reported lost or stolen.

1.5.17.4.2. This documentation must be scanned and stored in Defense Enrollment Eligibility Reporting System (DEERS). Inform the sponsoring organization of any change to the official relationship that served as the basis for access.

FOR OFFICIAL USE ONLY

1.5.17.5. Turn in access credentials to the issuance office or sponsoring organization when the credential expires or when the basis for obtaining the credential no longer exists.

1.5.17.6. Register their privately owned vehicle (POV) in accordance with Joint, Combatant Commander and installation guidance.

Chapter 2

INSTALLATION PERIMETER ACCESS CREDENTIALS

2.1. Source Documentation.

2.1.1. Per DoDI 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, and AFI 36-3026 (IP), Volume 1, the DoD provides members of the Uniformed Services with a distinct ID card identifying them as active duty, Guard, Reserve, or retired members and authorizing them to receive Uniformed Services' benefits and privileges.

2.1.2. The DoD also authorizes a distinct ID card for eligible family members and other individuals entitled to receive Uniformed Services' benefits and privileges, civilian affiliates (e.g. Red Cross employees), foreign affiliates (e.g. qualifying foreign military and foreign civilian liaisons), and a Service specific civilian ID card for DoD civilian employees and eligible contractor personnel.

2.1.3. In addition to DoD issued credentials, per DTM 09-012, *Interim Policy Guidance for DoD Physical Access Control*, the other non DoD credentials listed in this chapter are also authorized to facilitate access to Air Force installations.

2.2. Common Access Cards (CAC).

2.2.1. It is Department of Defense (DoD) policy that:

2.2.1.1. The CAC, a form of DoD ID card, shall serve as the Federal PIV card for DoD implementation of HSPD 12.

2.2.1.2. Per AFI 31-101, the CAC is the principal PIV credential used to facilitate physical access to facilities and installations.

2.2.2. The DoD is currently migrating the CAC in order to meet the Federal requirements for credentialing contained within HSPD-12 and Federal Information Processing Standards (FIPS) Publication 201-1, *Personal Identity Verification for Federal Employees and Contractors*.

2.2.2.1. Migration of the CAC will take place over multiple years as the card issuance hardware and software are upgraded.

2.2.2.2. CACs issued in conjunction with previous CAC policies, USD(P&R) DTM 08-003, and DTM 09-012 will remain valid until replaced with the next generation CAC.

2.2.3. HSPD-12 Implications. Office of Management and Budget Memorandum M-05-04, *Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, and DTM 08-003 define rules on the CAC and to whom it applies.

2.2.4. CAC Eligibility.

2.2.4.1. Automatic CAC Eligible Populations.

2.2.4.1.1. Specific populations are automatically eligible for a CAC based on their personnel category within the DoD.

FOR OFFICIAL USE ONLY

- 2.2.4.1.2. Examples include Uniformed Services personnel, DoD civilian employees, and specific categories of personnel assigned overseas in support of the Department.
- 2.2.4.2. Other Eligible CAC Populations.
- 2.2.4.2.1. CAC eligibility for other populations, including DoD contractors, non-DoD Federal Civilians, State employees, and other non-DoD affiliates, is based on the DoD government sponsor's determination of the type and frequency of access required to DoD facilities or networks that will effectively support the mission.
- 2.2.4.2.2. To be eligible for a CAC, the access requirement must meet one of the following criteria:
- 2.2.4.2.2.1. The individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the Department (applicable to DoD contractors only) on a recurring basis for a period of 6 months or more.
- 2.2.4.2.2.2. The individual requires both physical access to a DoD facility and access, via logon, to DoD networks on site or remotely. Access to the DoD network must require the use of a computer with Government-controlled configuration or use of a DoD-approved remote access procedure in accordance with the *Secure Remote Computing Security Technical Implementation Guide Version 1, Release 2*.
- 2.2.4.2.2.3. The individual requires remote access, via logon, to a DoD network using DoD-approved remote access procedures.
- 2.2.4.3. CAC eligibility for non-U.S. persons (non US Citizen/nonpermanent resident alien).
- 2.2.4.3.1. CAC eligibility for non-U.S. persons is based on DoD Government sponsorship.
- 2.2.4.3.2. Non-U.S. persons are eligible for CACs only if they meet one or more of the following:
- 2.2.4.3.2.1. Possess legal residence status within the United States for a minimum of 3 years, a favorable result from the Federal Bureau of Investigations fingerprint check, and an initiated National Agency Check with Written Inquiries (NACI) or equivalent investigation.
- 2.2.4.3.2.2. Possess a successfully adjudicated NACI or equivalent investigation.
- 2.2.4.3.2.3. Meet (as direct/indirect DoD hire personnel) the investigative requirements for DoD employment as recognized through international agreements pursuant to DoD 1400.25-M, *Civilian Personnel Manual*, Subchapter 1231, *Employment of Foreign Nationals*, and AFI 36-102, *Basic Authority and Responsibility for Civilian Personnel Management and Administration*.
- 2.2.4.3.2.4. Possess (as foreign military, employee, or contract support personnel) a visit status and security assistance that has been confirmed, documented, and processed in accordance with international agreements pursuant to DoD Directive 5230.20, *Visits and Assignment of Foreign Nationals*, AFI 16-107, *Military Personnel Exchange Program (MPEP)*, AFI 16-201, *Air Force Disclosure and*

Technology Transfer Program, and Air Force Policy Directive (AFPD) 16-1, International Affairs.

2.2.5. CAC Topology Specifications. CAC Stripe Color Coding. **Note:** If a person meets more than one condition below, priority will be given to the blue stripe to denote a non-U.S. citizen unless the card serves as a Geneva Conventions Card.

2.2.5.1. No Stripe. U.S. military and DoD civilian personnel or any personnel eligible for a Geneva Conventions card.

2.2.5.2. Blue. Non-U.S. personnel, including DoD contract employees (other than those persons requiring a Geneva Conventions card).

2.2.5.3. Green. All U.S. personnel under contract to the Department (other than those persons requiring a Geneva Conventions card).

2.2.5.4. Red. Reserved for First Responder personnel.

2.2.5.4.1. FIPS-201 reserves the color red to distinguish emergency first responder officials. However, policy governing the requirements for a first responder program has not been codified within the Department.

2.2.5.4.2. Until the DoD Implementation of HSPD-12 is complete, the color red will also be used to denote non-U.S. personnel in the same manner as the blue stripe.

2.2.6. CAC Printed Statements.

2.2.6.1. Eligible individuals who are permanently assigned in foreign countries for at least 365 days (it should be noted that local nationals are in their home country, not a foreign country) will have the word "OVERSEAS" printed within the authorized patronage area of the CAC.

2.2.6.2. The authorized patronage area for eligible individuals permanently assigned within the continental United States (CONUS) will be blank. Travel orders authorize access for these individuals while en-route to the deployment site.

2.2.6.3. The medical area on the card for individuals on permanent assignment in a foreign country will contain a statement, "When Temporary Assigned Duty/Temporary Duty (TAD/TDY) or stationed overseas on a space-available fully reimbursable basis." However, civilian employees and contractor employees providing support when forward deployed during a conflict, combat, or contingency operation are treated according to DoD Directive 1404.10, *DoD Civilian Expeditionary Workforce*, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, the Deputy Secretary of Defense Memorandum, *Policy Guidance for Provision of Medical Care for Department of Defense Civilian Employees Injured or Wounded While Forward Deployed in Support of Hostilities* and AFI 36-507, *Mobilization of the Civilian Work Force*.

2.2.7. Types of CAC Credentials. There are currently four CAC types that are used within the Department, based on cardholder eligibility. Each type will evolve into a next generation CAC type.

2.2.7.1. Armed Forces of the United States Geneva Conventions Card.

FOR OFFICIAL USE ONLY

Figure 2.1. Armed Forces of the United States Geneva Conventions Card.

2.2.7.1.1. This CAC is the primary ID card for active duty uniformed services members and shall be used to identify the member's eligibility for benefits and privileges administered by the uniformed services and shall also be used to facilitate standardized, uniform access to DoD facilities, installations and computer systems.

2.2.7.1.2. The following population categories are eligible for this CAC:

2.2.7.1.2.1. Members of the regular components of the Military Services.

2.2.7.1.2.2. Members of the Selected Reserve of the Ready Reserve of the Reserve Components.

2.2.7.1.2.3. Members of the Individual Ready Reserve of the Ready Reserve authorized according to regulations prescribed by the Secretary of Defense to perform duty in accordance with section 10147 of Title 10, U.S.C.

2.2.7.1.2.4. Military members of the Coast Guard, National Oceanic Atmospheric Administration (NOAA) and U.S. Public Health Service (USPHS).

2.2.7.1.3. Status area of the card will show the Agency/Department the individual is associated with for members on Active duty, and for members of the Selected Reserve not on active duty or full-time National Guard duty for 31 days or more.

2.2.7.1.4. This version of the CAC will be modified (from Armed Forces) to state "Uniformed Services" for members of the National Oceanic and Atmospheric Administration and the U.S. Public Health Service.

2.2.7.2. U.S. DoD and/or Uniformed Services ID Card.

FOR OFFICIAL USE ONLY

Figure 2.2. U.S. DoD and/or Uniformed Services ID Card.



2.2.7.2.1. This CAC is the primary ID card for Service Academy students, eligible civilian employees, contractors, and foreign national affiliates and shall be used to facilitate standardized, uniform access to DoD facilities, installations and computer systems.

2.2.7.2.2. DoD civilian employees are eligible for this CAC, to include:

2.2.7.2.2.1. Individuals appointed to appropriated fund and non-appropriated fund (NAF) positions (to include civilian employees of the U.S. Coast Guard and NOAA).

2.2.7.2.2.2. Permanent or time-limited employees on full-time, part-time, or intermittent work schedules for 6 months or more.

2.2.7.2.2.3. Senior Executive Service, Competitive Service, and Excepted Service employees.

2.2.7.2.3. Eligibility for additional populations shall be based on a combination of the personnel category and the DoD Government sponsor's determination of the type and frequency of access required to DoD networks and facilities. These personnel categories include:

2.2.7.2.3.1. Non-DoD civilian employees to include:

FOR OFFICIAL USE ONLY

- 2.2.7.2.3.1.1. NOAA civilian employees.
- 2.2.7.2.3.1.2. State employees working in support of the National Guard.
- 2.2.7.2.3.1.3. Intergovernmental Personnel Act employees.
- 2.2.7.2.3.1.4. DoD contractors.
- 2.2.7.2.3.1.5. NOAA Contractors.

2.2.7.2.3.2. Persons whose affiliation with DoD is established through:

- 2.2.7.2.3.2.1. Direct and Indirect Hiring Overseas. Non-U.S. citizens hired under an agreement with the host nation and paid directly by the Uniformed Services (direct hire) or paid by an entity other than the Uniformed Services for the benefits of the Uniformed Services (indirect hire).
- 2.2.7.2.3.2.2. Assignment as Foreign Military, Foreign Government Civilians, or Foreign Government Contractors to Support DoD Missions. Non-U.S. citizens who are sponsored by their government as part of an official visit or assignment to work with DoD.

2.2.7.3. U.S. DoD and/or Uniformed Services ID and Privilege Card.

Figure 2.3. U.S. DoD and/or Uniformed Services ID and Privilege Card.



2.2.7.3.1. This CAC is the primary ID card for civilian employees, contractors, and foreign national military, as well as other eligible individuals entitled to benefits and privileges administered by the uniformed services. The CAC shall be used to

FOR OFFICIAL USE ONLY

facilitate standardized, uniform access to DoD facilities, installations, and computer systems.

2.2.7.3.2. Specific population categories entitled to benefits and privileges are eligible for this CAC, to include:

2.2.7.3.2.1. DoD and uniformed services civilian employees (both appropriated and non-appropriated) when required to reside in a household on a military installation within the CONUS, Hawaii, Alaska, Puerto Rico, and Guam.

2.2.7.3.2.2. DoD and uniformed services civilian employees when stationed or employed and residing in foreign countries for a period of at least 365 days.

2.2.7.3.2.3. Other U.S. Government agency civilian employees when stationed or employed and residing in foreign countries for a period of at least 365 days.

2.2.7.3.2.4. DoD contractors when stationed or employed and residing in foreign countries for a period of at least 365 days.

2.2.7.3.2.5. DoD Presidential appointees who have been appointed with the advice and consent of the Senate.

2.2.7.3.2.6. Civilian employees of the Army and Air Force Exchange System, Navy Exchange System, and Marine Corps Exchange System and NAF activity employees of the Coast Guard Exchange Service.

2.2.7.3.2.7. Uniformed and non-uniformed full-time paid personnel of the Red Cross assigned to duty with the uniformed services within the CONUS, Hawaii, Alaska, Puerto Rico, and Guam, when required to reside in a household on a military installation.

2.2.7.3.2.8. Uniformed and non-uniformed, full-time, paid personnel of the Red Cross assigned to duty with the uniformed services in foreign countries.

2.2.7.3.2.9. Foreign military who meet specific eligibility requirements. Those foreign military not meeting the eligibility requirements for CAC shall be issued a DD Form 2765, *Department of Defense/Uniformed Services Identification and Privilege Card*.

2.2.7.3.2.10. Active duty officer and enlisted personnel of North Atlantic Treaty Organization (NATO) and Partnership For Peace countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department.

2.2.7.3.2.11. Active duty officer and enlisted personnel of non-NATO countries serving in the United States under the sponsorship or invitation of the Department of Defense or a Military Department.

2.2.7.3.2.12. Active duty officer and enlisted personnel of NATO and non-NATO countries when serving outside the United States and outside their own country under the sponsorship or invitation of the Department or a Military Department, or when it is determined by the major overseas commander that the granting of such privileges is in the best interests of the United States and such personnel are connected with, or their activities are related to, the performance of functions of

FOR OFFICIAL USE ONLY

the U.S. military establishment.

2.2.7.4. U.S. DoD and/or Uniformed Services Geneva Conventions ID Card for Civilians Accompanying the Armed Forces.

Figure 2.4. U.S. DoD and/or Uniformed Service Geneva Conventions ID Card for Civilians Accompanying the Armed Forces.



2.2.7.4.1. This CAC serves as the United States DoD and/or Uniformed Services Geneva Conventions ID card for civilians accompanying the Uniformed Services. The CAC shall be used to facilitate standardized, uniform access to DoD facilities, installations, and computer systems.

2.2.7.4.2. The following population categories are eligible for this CAC:

2.2.7.4.2.1. Emergency-essential employees as defined in DoD Directive 1404.10.

2.2.7.4.2.2. Contractors authorized to accompany the force (contingency contractor employees) as defined in Joint Publication 4-10, *Operational Contract Support*.

2.3. Non-Common Access Card (CAC) Department of Defense (DoD) Credentials. For eligible military, civilian (includes non-appropriated), and contractors, the CAC with the Integrated Circuit Chip (ICC) will replace the applicable ID card types below. For those personnel who do not receive a CAC, the credentials listed in this section are still authorized.

FOR OFFICIAL USE ONLY

2.3.1. Manually Produced Credentials. The DoD is in the process of eliminating manually generated credentials. Manually produced credentials do not have the capability to be electronically read/authenticated by a PACS. When this is fully implemented, the only credentials Air Force Security Forces will issue are locally produced PACS Passes/Cards and AF Form 75s. All other credentials will be issued via DEERS-RAPIDS.

2.3.1.1. If an individual presents a manually produced card at an installation, direct them to the local DEERS-Real-Time Automated Personnel Identification System (RAPIDS) card issuance facility to receive the appropriate/authorized machine readable card.

2.3.1.2. If the local DEERS-RAPIDS issuing official determines the individual is not eligible for a machine-readable credential, it will be up to the Installation Commander to determine whether or not a local PACS Pass/Card or AF Form 75 will be issued.

2.3.2. DD Form 2, *United States Uniformed Services Identification Card (Retired)* (Manually prepared card) or, DD Form 2, *United States Uniformed Services Identification Card (Retired)* (Machine-readable card). Eligibility category is as follows:

Figure 2.6. DD Form 2, *Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)*.

ARMED FORCES OF THE UNITED STATES	
DATE OF BIRTH 1976JAN02	RECEIVED BY [Signature]
[Barcode]	
DATE OF ISSUE 2011MAR02	BLOOD TYPE UNK
GENEVA CONV CATEGORY [Blank]	
[Barcode]	
DD FORM 2 (RESERVE) OCT 93 PROPERTY OF US GOVERNMENT	

2.3.3.1. Ready Reserve (Selected and Individual) and Standby Reserve. **Note:** Selected Reserve members receive a CAC. Individual and Standby Reserve, including Merchant Marine Academy, ROTC students, members with a military service obligation or separating or Retired Reserve awaiting retirement pay receive the DD Form 2 (Manually prepared or Machine-readable) card only.

2.3.3.2. ROTC students who receive educational assistance under Section 2107 of Title 10 and are enlisted in the Obligated Reserve Section. ROTC graduates appointed as members of a Reserve Component not on active duty orders for 31 consecutive days or more.

2.3.3.3. Members being released from active duty with a military service obligation (MSO). **Note:** Members departing on terminal leave with a MSO may use the DD Form 2 Reserve ID card along with their separation orders to obtain active duty benefits until their separation date.

2.3.3.4. Reserve Officers' Training Corps (ROTC) College Program students in their last 2 years of training.

2.3.3.5. Members involuntarily separating from the Selected Reserve under the Selected Reserve Transition Program (RTAP) and: (1) transferring to the Individual Ready Reserve or (2) Retired Reserve awaiting retirement pay who are eligible for benefits under the RTAP.

2.3.3.6. Merchant Marine Academy Midshipmen.

2.3.4. DD Form 2, *United States Uniformed Services Identification Card (Reserve Retired)* (Machine-readable card). Eligibility category is as follows:

FOR OFFICIAL USE ONLY

Figure 2.7. DD Form 2, *United States Uniformed Services Identification Card (Reserve Retired)*.

UNITED STATES UNIFORMED SERVICES

U.S. AIR FORCE
RESERVE RETIRED

DEPARTMENT OF THE AIR FORCE

RANK/PAY GRADE
MSGT E7

SIGNATURE
SAMPLE

EXPIRATION DATE
2011DEC31

DOD ID NUMBER

RESERVE, RETIREE
IDENTIFICATION CARD

DATE OF BIRTH
1952JAN01

PENSION NUMBER

DATE OF ISSUE
2011MAR01

MEDICAL
DISQUALIFIED

SAMPLE

CIVILIAN: NO

DD FORM 2 (RES. RET.) OCT 93 PROPERTY OF US GOVERNMENT

OUSD(P&R) OCT 2005

2.3.4.1. Members entitled to receive retirement pay.

2.3.4.2. Former members (discharged) entitled to receive retirement pay. The status “Former Member” will be reflected above the Service shield.

2.3.5. DD Form 1173, *Uniformed Services Identification and Privilege Card* (Manually prepared card); DD Form 1173, *United States Uniformed Services Identification and Privilege Card* (Machine-readable Card). Eligibility category is as follows:

FOR OFFICIAL USE ONLY

Figure 2.8. DD Form 1173, *Uniformed Services Identification and Privilege Card*.

2.3.5.1. Eligible family members of former (discharged) members entitled to receive retired pay.

2.3.5.2. Eligible surviving dependents of active duty members and surviving dependents of members entitled to retired pay.

2.3.5.3. Dependents of active duty members or Reservists on active duty in excess of 30 days, and dependents of members entitled to retired pay, including those members in a dual status, in the following categories:

2.3.5.3.1. Spouse.

2.3.5.3.2. Child under age 21.

2.3.5.3.3. Stepchild.

2.3.5.3.4. Ward.

2.3.5.3.5. Incapacitated child 21 years of age or older.

2.3.5.3.6. Full-time student between 21 and 23 years of age.

2.3.5.3.7. Parents, parents-in-law, stepparents, parents-by-adoption. **Note:** See Terms on Dual Status.

2.3.5.4. Eligible family members of Medal of Honor recipients and honorably discharged veterans rated by the VA as 100-percent disabled from a Uniformed Service-connected injury or disease, including eligible surviving dependents.

2.3.5.5. Eligible abused dependents of active duty members entitled to retired pay based on 20 or more years of service who are separated due to misconduct on or after 23 October 1992 and who lost their right to retired pay, 10 U.S.C. 1408(h).

2.3.5.6. Eligible dependents of active duty members (over 30 days) not entitled to retired pay who were separated from active duty or forfeited all pay and allowances under a court-martial sentence resulting from a dependent abuse offense or administratively separated from active duty, and the basis for separation includes a dependent-abuse

FOR OFFICIAL USE ONLY

offense when separated on or after 30 November 1993, and when dependents are eligible for transitional privileges.

2.3.5.7. Accompanying family members of foreign personnel living with the sponsor in certain instances.

2.3.5.8. Eligible family members of civilian personnel members in certain instances.

2.3.5.9. Eligible family members of involuntarily separated members eligible under Transition Assistance Management Program (TAMP) or Transition Assistance (TA). Eligible family members of voluntarily separated member are eligible under the Special Separation Benefit (SSB) and Voluntary Separation Incentive (VSI) programs.

2.3.5.10. Eligible dependents of Philippine Scouts who have applied for benefits under Public Law 77-140 (1941) and Public Law 79-51 (1945).

2.3.5.11. Qualified dependents under 10 years of age if:

2.3.5.11.1. The child does not reside in the household of an eligible adult ID card holder (permanently or temporarily).

2.3.5.11.2. The child is of a joint Service married couple.

2.3.5.11.3. The child is a child of a single parent.

2.3.5.11.4. The child's physical appearance warrants issue (i.e., child looks over 10 years old).

2.3.5.11.5. As authorized by the issuance facility Site Security Manager or Verifying Official due to unique or extenuating circumstances.

2.3.6. DD Form 1173-1, *Department of Defense Guard and Reserve Dependent Identification Card* (Manually prepared card) or *Department of Defense Guard and Reserve Dependent Identification Card* (Machine-readable card). Eligibility category is as follows:

Figure 2.9. DD Form 1173-1, *Department of Defense Guard and Reserve Dependent Identification Card*.

UNITED STATES UNIFORMED SERVICES		DATE OF BIRTH	BENEFITS NUMBER
 SAMPLE	EXPIRATION DATE	1984JAN03	
	SPONSOR SERVICE/STATUS	[Barcode]	
	SPONSOR RANK/PAY GRADE	DATE OF ISSUE	MEDICAL
	RELATIONSHIP	2011MAR07	SAMPLE
SIGNAL TYPE	SPONSOR	DUTY ORDERS	
SPOUSE, NG	NATIONAL GUARD	30 DAYS	
IDENTIFICATION AND PRIVILEGE CARD		[Barcode]	
		DD FORM 1173-1	OCT 93
		PROPERTY OF US GOVERNMENT	

2.3.6.1. Eligible dependents of Reserve component members not on active duty in excess of 30 days in the following categories:

2.3.6.1.1. Spouse.

FOR OFFICIAL USE ONLY

- 2.3.6.1.2. Child under age 21.
- 2.3.6.1.3. Stepchild.
- 2.3.6.1.4. Ward.
- 2.3.6.1.5. Incapacitated child 21 years of age and older.
- 2.3.6.2. Full-time student between 21 and 23.
- 2.3.6.3. Parents/Parents-in-law, stepparents, and parents-by-adoption.
- 2.3.6.4. Eligible dependents of Ready Reserve and Standby members and Gray Area retirees as part of the Guard and/or Reserve DEERS Enrollment Program.
- 2.3.6.5. Eligible dependents of former members when the former member is eligible for retired pay.
- 2.3.6.6. Eligible surviving dependents of Retired Reserve members entitled to pay at age 60, who died before attaining that age. Issue the DD Form 1173-1 until member would have attained age 60. **Note:** (The DD Form 1173 may be issued only on or after the date on which the member would have been 60 years old, had he or she survived, regardless if this member would have been eligible before age 60 for retirement pay).
- 2.3.6.7. Eligible surviving dependents of Reserve members who had earned 20 qualifying years for retirement and are in receipt of their Notice of Eligibility for Retirement Pay at age 60, who had not reached age 60, and had not transferred to the Retired Reserve, and who died prior to reaching age 60. **Note:** The DD Form 1173-1 is issued until the member would have been 60 years old, had he or she survived. The DD Form 1173 is issued only on or after the member would have been 60 years old had he or she survived, regardless if this member would have been eligible before age 60 for retirement pay.
- 2.3.6.8. Eligible surviving dependents of former members who have met time-in-service requirements for retired pay at age 60, were discharged and are in receipt of their Notice of Eligibility for Retirement Pay at age 60, who had not reached age 60, and who died prior to reaching age 60.
- 2.3.6.9. Members involuntarily separating from the Selected Reserve, eligible for Selected Reserve Transition Program benefits due to discharge to civilian status on or after 23 October 1992 but before 31 December 2001 and eligible dependents.
- 2.3.6.10. Members involuntarily separating from the Selected Reserve eligible for Selected Reserve Transition Program benefits and transferring to the Individual Ready Reserve or Retired Reserve members awaiting retirement pay, on or after 23 October 1992 but before 31 December 2001 and eligible dependents.
- 2.3.6.11. Qualified dependents under 10 years of age if:
 - 2.3.6.11.1. The child does not reside in the household of an eligible adult ID card holder (permanently or temporarily).
 - 2.3.6.11.2. The child is of a joint service married couple.
 - 2.3.6.11.3. The child is a child of a single parent.

FOR OFFICIAL USE ONLY

2.3.6.11.4. The child's physical appearance warrants issue (i.e., child looks over 10 years old).

2.3.7. DD Form 1934, *Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces* (Manually prepared card). **Note:** The Defense Human Resource Activity (DHRA) is converting the manually produced form to a machine readable form. Once this is complete, the manually prepared card will be cancelled. Until then, this credential will be issued in addition to an existing military or civilian Geneva Conventions CAC. If using PACS, entry controllers will validate either the machine readable DD Form 1934 or the other machine readable credential the person possesses for electronic authentication. Eligibility category is as follows:

Figure 2.10. DD Form 1934, *Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces*.

LOSS OF THIS CARD MUST BE REPORTED AT ONCE

UNITED STATES OF AMERICA
DEPARTMENT OF DEFENSE
WASHINGTON, D.C.

GENEVA CONVENTIONS

IDENTITY CARD
FOR MEDICAL AND RELIGIOUS PERSONNEL WHO
SERVE IN OR ACCOMPANY THE ARMED FORCES

LAST NAME - FIRST NAME - MIDDLE NAME
SAMPLE

CAPACITY

RANK

SOCIAL SECURITY NO.

ISSUING OFFICER

SIGNATURE OF BEARER

PROPERTY OF THE U.S. GOVERNMENT

HEIGHT	WEIGHT	COLOR HAIR	COLOR EYES

RELIGION	MARITAL STATUS	DATE OF BIRTH

CARD SERIAL NO. **SAMPLE** DATE ISSUED

NOTICE: THE PERSON WHOSE SIGNATURE, PHOTOGRAPH AND FINGERPRINTS APPEAR HEREON IS PROTECTED BY THE GENEVA CONVENTIONS FOR THE AMELIORATION OF THE CONDITION OF WOUNDED AND SICK IN THE ARMED FORCES IN THE FIELD, AND AT SEA OF AUGUST 12, 1949. IF THE BEARER SHALL FALL INTO THE HANDS OF AN ENEMY OF THE UNITED STATES HE SHALL AT ONCE SHOW THIS CARD TO THE DETAINING AUTHORITIES TO ASSIST IN HIS IDENTIFICATION. WHILE RETAINED HE IS ENTITLED AS A MINIMUM TO THE BENEFITS AND PROTECTIONS EXTENDED TO PRISONERS OF WAR OF EQUIVALENT RANK.

POSTMASTER: RETURN TO
AFMPC/DPWD
RAFS TX 318

2.3.7.1. Medical personnel.

2.3.7.2. Religious personnel.

2.3.7.3. Auxiliary medical personnel who serve in or accompany the military forces of the US in areas of combat and who are liable to capture and detention by the enemy as prisoners of war.

FOR OFFICIAL USE ONLY

2.3.7.4. The DD Form 1934, is issued in addition to an existing military or civilian Geneva Conventions CAC.

2.3.8. *DD Form 2764, United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card (Machine-readable card).* **Note:** The CAC replaces the *DD Form 489* and *DD Form 2764* for CAC eligible personnel; non-CAC eligible personnel may qualify for the *DD Form 2764*. Current Eligibility Category is as follows – **Note:** any additional eligibility categories must be approved by DHRA.

Figure 2.11. DD Form 2764, United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card.

UNITED STATES DOD/UNIFORMED SERVICES CIVILIAN		DATE OF BIRTH 1945JAN01
EXPIRATION DATE 2014MAR02		[Barcode]
SERVICE / ORGANIZATION KSMC /		
STATUS / GRADE FN/E7		DATE OF ISSUE 2011MAR03
MEDICAL NOT ELIGIBLE FOR DIRECT CARE PRIVILEGES		BLOOD TYPE UNK
DOD ID NUMBER		GENEVA CONV CATEGORY
SIGNATURE SAMPLE		[Barcode]
AFFILIATE, MILITARY KSC		
GENEVA CONVENTIONS IDENTIFICATION CARD		

DD FORM 2764 APR 1998 PROPERTY OF US GOVERNMENT

2.3.8.1. Korean Service Corps (Foreign Affiliate Military)

2.3.9. *DD Form 2765, Department of Defense/Uniformed Services Identification and Privilege Card (Machine readable card).* Eligibility category is as follows:

Figure 2.12. DD Form 2765, Department of Defense/Uniformed Services Identification and Privilege Card.

DEPARTMENT OF DEFENSE/UNIFORMED SERVICES		DATE OF BIRTH 1951JAN07
EXPIRATION DATE INDEF		[Barcode]
SERVICE / ORGANIZATION USN /		
STATUS / GRADE DAVPRM/E5		DATE OF ISSUE 2011FEB01
MEDICAL SAMPLE		CIVILIAN: NO
DOD ID NUMBER		[Barcode]
SIGNATURE SAMPLE		
Name		
IDENTIFICATION AND PRIVILEGE CARD		

DD FORM 2765 APR 1998 PROPERTY OF US GOVERNMENT

2.3.9.1. Medal of Honor recipients and honorably discharged veterans rated by the VA as 100-percent disabled from a Uniformed Service-connected injury or disease (other than current or retired members of the Uniformed Services).

FOR OFFICIAL USE ONLY

2.3.9.2. Un-remarried and unmarried former spouses determined eligible for continued benefits under the Uniformed Services Former Spouse Protection Act.

2.3.9.3. Former members entitled to receive retired pay. Former member refers to an individual who is in receipt of retired pay for non-Regular service under Chapter 1223 of 10 U.S.C., who has been discharged from the Service, and who maintains no military affiliation.

2.3.9.4. Civilian personnel in the following categories:

2.3.9.4.1. Contract surgeons overseas during the period of their contract.

2.3.9.4.2. Uniformed and non-uniformed full-time paid personnel of the Red Cross assigned to duty with the Uniformed Services within the CONUS, Hawaii, Alaska, Puerto Rico and Guam when required to reside in a household on a military installation. **Note:** This category will now receive a CAC in place of the DD Form 2765.

2.3.9.4.3. Uniformed and non-uniformed full-time paid personnel of the Red Cross assigned to duty with the Uniformed Services in foreign countries. **Note:** This category will now receive a CAC in place of the DD Form 2765.

2.3.9.4.4. Area executives, center directors, and assistant directors of the United Service Organizations (USO), when serving in foreign countries.

2.3.9.4.5. United Seaman's Service (USS) personnel in foreign countries.

2.3.9.4.6. Civilian personnel of the Department of Defense and the Uniformed Services, when required to reside in a household on a military installation within the Continental United States (CONUS), Hawaii and, Alaska.

2.3.9.4.7. Civilian personnel of the Department of Defense, the Uniformed Services, and other Government Agencies, and civilian personnel under private contract to the Department of Defense or a Uniformed Service, when stationed or employed in foreign countries or when stationed or employed in Puerto Rico or Guam, and their accompanying dependents, when residing in the same household.

2.3.9.5. Military Sealift Command (MSC) civil service marine personnel deployed to foreign countries on MSC-owned and operated vessels.

2.3.9.6. Ship's officers (civilian employees, not commissioned officers) and members of the crews of vessels of the NOAA (Title 33 U.S.C. 857-4).

2.3.9.7. Officers and crews of vessels, lighthouse keepers and depot keepers of the former Lighthouse Service.

2.3.9.8. Involuntarily separated members eligible for TA benefits. These individuals shall be issued a DD Form 2765 (with a TA over stamp) showing expiration date for the medical benefit, as shown on the reverse of the card.

2.3.9.9. Non-sponsored NATO personnel in the United States. Active duty officer and enlisted personnel of NATO countries who, in connection with their official NATO duties, are stationed in the United States and are not under the sponsorship of the

Department of Defense or a Military Department, are not eligible for a CAC, and will continue to received a DD Form 2765.

2.3.10. *Civilian Retiree Card.* Eligibility category is Civilians who retire from any DoD Service Component or Agency:

Figure 2.13. *Civilian Retiree Card.*



2.3.10.1. In accordance with DoD Morale, Welfare, and Recreation (MWR) policy, limited use of military MWR activities are permitted at the discretion of the installation commander.

2.3.10.2. The installation commander retains the authority to restrict access to MWR facilities for reasons such as local demand, facility capacity, and security concerns.

2.3.10.3. Installations will only grant access if the installation commander has approved the individual MWR privileges to his/her particular installation.

2.4. Non-Department of Defense (DoD) Federal Personal Identity Verification (PIV). HSPD-12 “Policy for a Common Identification Standard for Federal Employees and Contractors,” requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. Per the Office of Management and Budget Memorandum M-05-04, *Implementation of HSPD 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 5, 2005, the directive applies to “Executive departments” and agencies listed in title 5 U.S.C. § 101, the Department of Homeland Security; “independent establishments” as defined by title 5 U.S.C. §104(1); and the United States Postal Service (title 39 U.S.C § 201).

FOR OFFICIAL USE ONLY

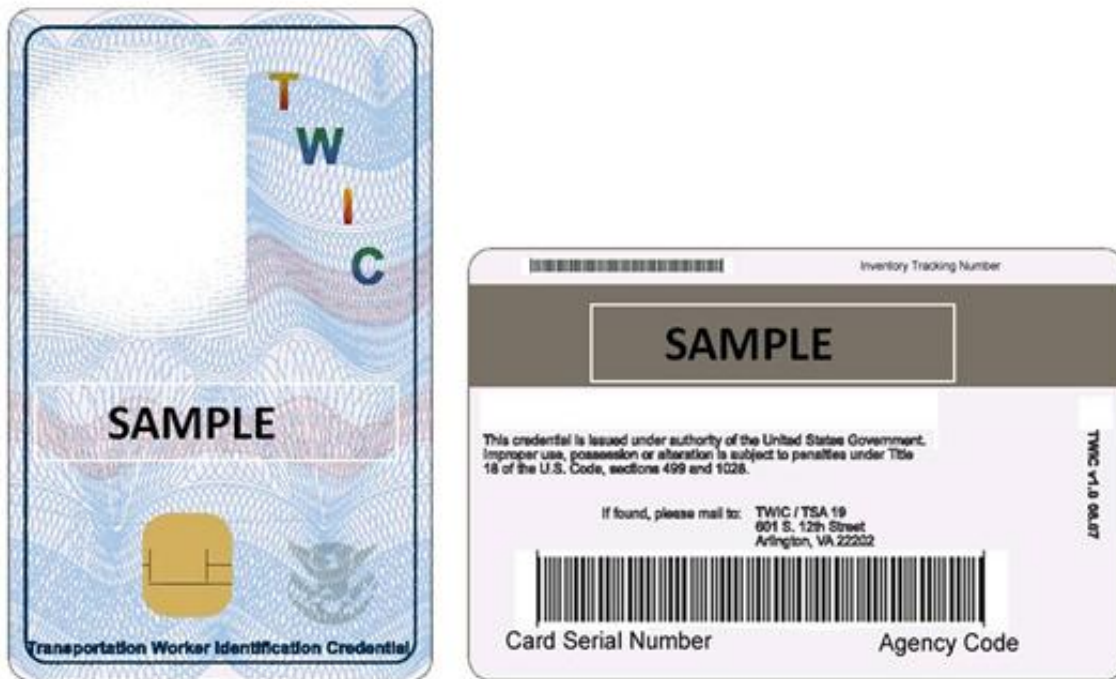
2.4.1. Non-DoD Federal PIVs include HSPD-12 compliant credentials from the Department of State, Department of Treasury, Department of Justice, Department of the Interior, Department of Agriculture, Department of Commerce, Department of Labor, Department of Health and Human Services, Department of Housing and Urban Development, Department of Transportation, Department of Energy, Department of Education, Department of Veterans Affairs, Department of Homeland Security and the United States Postal Service.

2.4.2. An example of a Department of Homeland Security Federal PIV is located at Figure 2.14.

Figure 2.14. DHS Federal PIV.



2.5. Transportation Worker Identification Credential (TWIC). TWIC was established by Congress through the Maritime Transportation Security Act (MTSA) and is administered by the Transportation Security Administration (TSA) and U.S. Coast Guard. TWICs are tamper-resistant biometric credentials that will be issued to workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities and all credentialed merchant mariners.

Figure 2.15. TWIC.

2.6. Personal Identity Verification-Interoperable (PIV-I). Non-federal organizations have expressed a desire to issue identity cards that are technically interoperable with Federal government PIV systems, and issued in a manner that allows Federal government relying parties to trust the cards.

2.6.1. PIV-I benefits. A PIV-I credential, where accepted by the relying party (installation commander or a DoD information system owner), provides a fraud resistant, federally interoperable, and electronically validated identity solution for populations of DoD mission partners and commercial vendors that interact with the DoD on a recurring basis. Generally, use of PIV-I credentials, wherever possible, reduces overhead costs of issuing additional credentials, where still ensuring appropriate security, risk management, and identity proofing and vetting.

2.6.2. Qualified PIV-I Credentials. For DoD vendors to use PIV-I credentials to access DoD information systems or facilities, they should procure qualified PIV-I credentials from credential providers that have been approved in accordance with the DoD External Interoperability Plan.

2.6.3. PIV-I for installation perimeter access control. The use of PIV-I for installation perimeter access control is authorized if an installation has an electronic PACS that is deployed and operational, the PIV-I credential is electronically authenticated and a basic name check is conducted through the National Crime Information Center (NCIC). Please see section 5.2.1.2. for information on an NCIC Name Check.

2.7. Locally Produced Physical Access Control System (PACS) Passes/Cards and AF Form 75 Visitor Pass/Vehicle Pass. Individuals receiving a locally produced credential must have a validated need to enter the installation and be properly sponsored. The individual must submit to

FOR OFFICIAL USE ONLY

applicable identity proofing, vetting and fitness determination; and conform to USAF protocol requirements for physical access and credential/screening standards as specified in this AFI. The PACS pass/card will provide access only at the base issued, unless regional/CONUS partnerships are established and agreed upon for reciprocation of use and access authorization among Installations/Services. Access authorizations may vary based on needs and requirements of the installation. One-time, intermittent, or recurring access to installations is at the will of the Installation Commander.

2.7.1. Eligible Populations. Populations requiring one-time, intermittent, or routine installation access may include, but are not limited to, contractors, employees, volunteers, visitors (official and unofficial), delivery organizations, service providers, vendors, interns, DoD civilian retirees, Honorary Commanders, and privatized housing occupants. Individuals may or may not be US citizens.

2.7.2. The credential can be revoked for cause at any time based on the actions of the individual or the sponsor.

2.7.3. PACS Pass/Card Standards. Individuals requiring access for 1-60 days should be issued a PACS pass. Individuals requiring access for greater than 60 days should be issued a PACS card. All locally produced PACS passes/cards, as a minimum, will include:

2.7.3.1. Person's full legal name (first, middle, and last name).

2.7.3.2. Person's descriptive information (gender, height, weight, color hair, color of eyes).

2.7.3.3. Current facial image/digital photograph.

2.7.3.4. Fingerprints.

2.7.3.5. Affiliation (Employee, Contractor, Vendor, Visitor, etc.).

2.7.3.6. Agency/Organization Issuer.

2.7.3.7. Pass/card serial number.

2.7.3.8. Sponsor identification.

2.7.3.9. Expiration date.

2.7.3.10. Time group (as appropriate if an individual is only authorized on the installation during certain hours).

2.7.3.11. Bar code to allow for electronic interrogation to ensure the credential is valid and the person has authorization to enter (if using PACS).

2.7.3.12. Time, date, and event/emergency access restrictions.

2.7.3.13. Unique identifier for visual pass/card authenticity determination.

2.7.3.14. Escort Authority and Restrictions.

2.7.3.15. FPCON level authorization.

2.7.3.16. An example of a locally produced PACS (Defense Biometrics Identification System – DBIDS) card is located at figure 2.16.

Figure 2.16. DBIDS Card.

Presidio of Monterey - Personal Employee			
	APPROVED ACCESS	EXPIRES	
	0001-2400	2003	
	MON-SUN	OCT15	
AREA OF ACCESS	Force Protection Condition		
DLI	A		
ONLY	RANK/GRADE		
SSN		ESCORPT PRIVILEGE	
Name		NO PERSON OR VEHICLE ESCORTS *	
Defense Language Institute Foreign Language Center			

DATE OF BIRTH	WEIGHT	HEIGHT	HAIR COLOR	EYE COLOR
1970Feb02	150	64	AU	HZ
				
REMARKS				
training card only!!!!				
SAMPLE				
			IF FOUND, PLEASE RETURN TO THE PRESIDIO OF MONTEREY	
DATE ISSUED 2002Oct15			PROPERTY OF US ARMY	

2.7.4. AF Form 75. Installations may continue to use the AF Form 75 as an access credential to USAF installations until PACS are installed.

2.7.4.1. A picture will be taken and affixed to rear of the pass listed as “FOR LOCAL USE.”

2.7.4.2. The visitor’s descriptive information from identity proofing source documents will be listed beneath the picture in the “FOR LOCAL USE” block.

2.7.4.3. Authorized base access dates, times, and other FPCON or emergency restrictions will be placed in the “TOTAL NUMBER IN PARTY” block.

2.7.4.4. The AF Form 75, and all local passes issued without a barcode that can be read electronically, should be laminated after a unique authenticator is placed on the credential (local stamp overlapping the picture and pass prior to lamination, infrared (IR) stamp, number authenticator, etc.) and will be carried by the visitor at all times while on the installation. The possession of the pass will signify that all processing actions (sponsorship/need determination, identity proofing, vetting, and vehicle screening) have been completed by the SF issuance agency.

2.7.5. Accountability of Locally Produced PACS Passes/Cards and AF Form 75s. Issuance facilities must be able, in near real-time, to track issued active and expired locally produced PACS passes/cards and AF Form 75s.

2.7.5.1. Issuance facilities will develop procedures to collect expired credentials from the sponsoring organizations/members when visits are complete. The procedures should be established and published in the IDP. Installations will develop a training and certification plan for those authorized to issue installation visitor credentials.

2.7.5.2. All passes issued will be maintained in a log or database to ensure visitor accountability during emergencies or exigent circumstances.

2.8. Approved Department of Defense (DoD) Privilege Card Holders.

2.8.1. DoDI 1330.21, *Armed Service Exchange Regulations*, and AFI 34-211(I), *Army and Air Force Exchange Service Operations*, authorizes exchange privileges for certain credential

FOR OFFICIAL USE ONLY

holders (e.g., US Coast Guard Auxiliary), but these credentials are not authorized to facilitate unsponsored or unescorted entry to DoD installations.

2.8.2. Credential holders who possess a DoD approved credential that authorizes exchange privileges, but not installation access, may be granted access to an installation if sponsored onto the installation by authorized individuals or organizations; or via an authorized escort.

2.8.3. Installations will codify access control procedures for approved DoD Privilege Card Holders in local instructions to ensure these personnel receive the appropriate benefits as mandated in DoDI 1330.21 and AFI 34-211(I).

2.9. Veterans Identification Card (VIC).

Figure 2.17. Veterans Identification Card.



2.9.1. The Department of Veterans Affairs provides eligible Veterans a Veterans Identification Card (VIC) for use at Veterans Affairs (VA) Medical Facilities. Only Veterans who are eligible for VA medical benefits will receive the card. The card will only display the Veteran's name, picture, and special eligibility indicators (e.g. Service Connected, Purple Heart and Former Prisoner of War (POW)) on the front of the card, if applicable.

2.9.2. The VIC is only used for the purpose of identification and check-in for VA appointments, and does not by itself facilitate access to installations.

FOR OFFICIAL USE ONLY

2.9.3. Eligible Veterans will provide the VIC at Installation Visitor Center's with VA Medical Facilities located on them to validate eligibility to receive a local pass/card or AF Form 75.

2.9.4. Installations will codify access control procedures for this category of personnel in applicable access control plans.

2.10. Privatized Housing.

2.10.1. Personnel associated with privatized housing are authorized the following credentials based on their assigned category:

2.10.1.1. Category 1 – Project Owner Corporate/Regional Personnel (sponsored by AFCEE/HP). Category 1 personnel are issued a CAC. Category 1 personnel will be considered in the contractor category and will have a green stripe.

2.10.1.2. Category 2 – Project Owner Property Management/Maintenance Personnel (sponsored by the Base's Capital Asset Manager). Category 2 personnel are issued a locally produced credential.

2.10.1.3. Category 3 – Project Owner Contractors/Subcontractors (sponsored by the Base's Capital Asset Manager). Category 3 personnel are issued a locally produced credential.

2.10.1.4. Category 4 – Eligible Tenants/Housing Occupants (sponsored by the Base's Capital Asset Manager). Category 4 personnel are issued a locally produced credential.

2.10.2. Geographically Separated Privatized Housing Subcontractor Screening. For geographically separated privatized housing areas where access is not controlled through the use of identification media, except potentially during higher FPCONs, subcontractor screening procedures are still required.

2.11. Air Force Office of Special Investigation (AFOSI) Special Agents.

2.11.1. AFOSI Agents are issued rank-neutral PACS credentials or CACs as they become available.

2.11.2. When such cards are presented with special agent credentials, after electronic authentication via a PACS that the credential is valid and the person is fit, AFOSI agents will have unescorted access to the installation and escort privileges for personnel and official vehicles in all force protection conditions.

2.12. Federal Bureau of Investigation (FBI) and United States Secret Service (USSS) Special Agents.

2.12.1. FBI and USSS Agents are issued rank-neutral PACS credentials or Federal PIV cards as they become available.

2.12.2. When such cards are presented with special agent credentials, after electronic authentication via a PACS that the credential is valid and the person is fit, FBI and USSS agents will have unescorted access to the installation and escort privileges for personnel and vehicles in all force protection conditions.

FOR OFFICIAL USE ONLY

Chapter 3

IDENTITY PROOFING AND REGISTRATION

3.1. Identity Proofing Concept. Once the need for installation physical access is established, the USAF will employ the following baseline standards for identity proofing (the process of providing sufficient information (e.g., identity history, credentials, documents) when attempting to establish an identity).

3.1.1. Without successful identity proofing, screening of professed identities is ineffective. Any registration information provided by applicants will be done so voluntarily with full applicant knowledge regarding the types of information to be collected, understanding of the purpose of collection, how the information may be shared, how the information will be protected, and the complete set of uses for the installation access credential/token (if issued) and its information. Lack of successful identity proofing may result in denial of access to the installation.

3.1.2. Only personnel delegated by the installation commander shall perform identity proofing. Delegation will be in writing, either by position designation codified in local guidance or name.

3.2. Common Access Card (CAC) Populations. Identity proofing requirements for CAC populations is prescribed in DTM 09-012. Persons possessing a CAC issued card IAW DTM 08-003 are identity proofed at card issuance sites from Federally authorized identity documents and shall be considered identity proofed.

3.3. Non-Common Access Card (CAC) Department of Defense (DoD) Populations. Identity proofing requirements for military, retiree/dependent, civilian (included non-appropriated) and contractor populations are prescribed in DTM 09-012. Persons possessing a DoD issued card IAW DTM 09-012 and AFI 36-3026 (IP), Volume 1, are identity proofed at card issuance sites from Federally authorized identity documents and shall be considered identity proofed.

3.4. Non-Department of Defense (DoD) Federal Personal Identity Verification (PIV) Populations. Persons possessing Federal PIV credentials that conform to DTM 09-012 are vetted and adjudicated by government security specialists on a NACI or Office of Personnel Management (OPM) Tier I standards (when implemented), and shall be considered identity proofed.

3.5. Transportation Worker Identification Credential (TWIC) Holders. TWIC holders vetting, adjudication, and issuance process is comparable to the NACI and/or National Agency Check with Law and Credit or OPM Tier I standards (when implemented), and shall be considered identity proofed.

3.6. Personal Identity Verification-Interoperable (PIV-I) Credentials. Approved PIV-I issuers have to meet the federal bridge certification to ensure their identity proofing standards are comparable to DoD standards, thus the PIV-I is considered identity proofed, and additional identity proofing is not required. Vetting via an NCIC name check and the Terrorist Screening Database (TSDB), when available, is still required.

3.7. Locally Produced Physical Access Control System (PACS) Passes/Cards and AF Form 75 Visitor Pass/Vehicle Pass. Personnel that do not possess a credential authorized to facilitate

FOR OFFICIAL USE ONLY

access and have a validated need for one-time, intermittent or routine unescorted physical access to an installation, and have been properly sponsored, require identity proofing and vetting to determine fitness and eligibility for access. **Note:** SF are authorized to provide local PACS credentials to AFOSI, FBI and USSS agents.

3.7.1. Persons requesting access shall provide justification and/or purpose for access to DoD installations/facilities. USAF installations, through implementing instructions, will ensure they have a valid means of identifying and verifying need for installation access, which may include, but are not limited to:

3.7.1.1. DoD intent to employ or employment of contractors, interns, and other members.

3.7.1.2. Sponsorship (please see section 6.6. for information on sponsorship).

3.7.1.3. DoD sponsorship of foreign military members, foreign civilians and in certain accompanied circumstances, their families, is accomplished in an official capacity through the DoD FVS or other DoD mechanisms pursuant to DoDD 5230.20, AFI 16-107, AFI 16-201, and AFPD 16-1.

3.7.1.3.1. FVS-CM is a software application developed to track and confirm foreign visitors at all DoD component installations. The software is CITRIX-based for users to access anywhere with Non-classified Internet Protocol Router Network (NIPRNET) connectivity and for those who have been trained and have a user name and password.

3.7.1.3.2. Within FVS and through the use of the FVS-CM, DoD and unit sponsors will validate need for access and assure identity proofing and vetting in accordance with DoD implementing guidance, and account for foreign nationals on DoD-sponsored official visits.

3.7.1.3.3. Records also must be maintained of foreign visits that have not been processed through the FVS. Accordingly, the USAF will record all visits or assignments of foreign nationals to their installations. It is the sponsoring organization's responsibility to ensure the visit is properly recorded and documented in the DoD FVS; and the local AFOSI unit is notified when official foreign visitors arrive and depart the installation.

3.7.2. Persons requesting access that are not in possession of an approved, government issued card, shall provide approved forms of ID proofing listed in section 3.7.6. The documents presented shall be reviewed by an authorized government representative for the purposes of identity proofing. Any fraudulent information passed during the process may lead to prosecution under appropriate legal authorities.

3.7.3. Prior to acceptance, SF will visually and tactilely (by touch or feel) screen documents for evidence of tampering, alteration, or other indications of falsified/fraudulent documents. Officials will not accept documents that appear to be fraudulent, forged, or counterfeit. SF will:

3.7.3.1. Pay attention to strange text, fonts, slightly altered text, incomplete letters, misaligned words, strange spacing and errors in punctuation and spelling.

3.7.3.2. Feel whether a photo has been glued over the original.

FOR OFFICIAL USE ONLY

3.7.4. ID illuminators. These lights illuminate hidden security features on identification and employment eligibility documents and expose hidden security features on IDs and should be employed if available.

3.7.5. Local implementation standards will include response actions, to include detention, for persons attempting to provide fraudulent documents for the purpose of defeating identity proofing procedures. If available and practicable, MAJCOMs and installations, in accordance with their assumption of risk, may choose to employ methods of electronic interrogation of these forms to ensure the highest confidence in their authenticity.

3.7.6. One form of the following documents will be accepted as proof of identity. The document must be a picture ID and all documents must be unexpired and valid. The goal is to minimize, within acceptable risk, the potential of improper screening and access credential issuance. **Note:** The information in section 3.7.6.1. – 3.7.6.7. is from *Handbook for Employers, Instruction for Completing Form I-9 (Employment Eligibility Verification Form)*, U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services.

3.7.6.1. United States Passport. The U.S. Department of State issues the U.S. Passport to U.S. citizens and nationals.

Figure 3.1. United States Passport.



3.7.6.2. Permanent Resident Card/Alien Registration Receipt Card (Form I-551).

FOR OFFICIAL USE ONLY

Figure 3.2. Permanent Resident Card/Alien Registration Receipt Card (Form I-551).



3.7.6.2.1. The Permanent Resident Card shows the DHS seal and contains a detailed hologram on the front of the card. Each card is personalized with an etching showing the bearer's photo, name, fingerprint, date of birth, alien registration number and card number.

3.7.6.2.2. Also in circulation are older Resident Alien cards, issued by the U.S. Department of Justice, Immigration and Naturalization Service, which do not have expiration dates and are valid indefinitely. These cards are peach and show the Department of Justice seal, and the bearer's fingerprint and photograph.

3.7.6.3. A foreign passport with a temporary (I-551) stamp or temporary (I-551) printed notation on a machine readable immigrant visa.

FOR OFFICIAL USE ONLY

Figure 3.4. An employment authorization document that contains a photograph (Form I-766).



3.7.6.4.1. USCIS issues the Employment Authorization Document to aliens granted temporary employment authorization in the United States.

3.7.6.4.2. The card contains the bearer's photograph, fingerprint, card number, Alien number, birth date, and signature, along with a holographic film and the DHS seal. The expiration date is located at the bottom of the card.

FOR OFFICIAL USE ONLY

3.7.6.5. A current/valid driver's license or identification card issued by a state or outlying possession of the United States provided it contains a photograph and biographic information such as name, date of birth, gender, height, weight, eye color and address.

Figure 3.5. Current/Valid Driver's License.



3.7.6.6. Identification card issued by Federal, State, or local government agencies, provided it contains a photograph and biographic information such as name, date of birth, gender, height, eye color, and address.

[illegible]

3.7.6.7. U.S. Coast Guard Merchant Mariner Cards/Credentials.

FOR OFFICIAL USE ONLY

Figure 3.7. U.S. Coast Guard Merchant Mariner Legacy Cards.



FOR OFFICIAL USE ONLY

Figure 3.8. U.S. Coast Guard New Merchant Mariner Credential.



3.7.6.7.1. New credential will look and feel exactly like a passport. The cover will be embossed with holographic images, invisible until exposed to Ultraviolet (UV) light. **Note:** Due to scanning constraints, the color depicted on the cover is not a true color match. The actual color is slightly lighter red/orange.

3.7.6.7.2. The paper stock will contain unique watermarks, visible red and blue fibers and invisible fluorescent fibers. Hand-drawn artwork, unique fonts, and UV reactive inks are just a few of the security features found in the paper and design of the credential.

FOR OFFICIAL USE ONLY

3.7.7. In addition to the above identity proofing documents, parents/legal guardians may provide any of the following credentials for the purpose of identity proofing for persons under the age of 18 who do not possess a photo ID. **Note:** Installation Commanders will determine the identity proofing and vetting requirements for minors under the age of 18 based on asset criticality, local threat, vulnerability, and assumption of risk.

3.7.7.1. School record or report card.

3.7.7.2. Day care or nursery school record.

3.7.7.3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal.

3.7.8. Additional supplemental sources of identity proofing (to be used in concert with the documents above to further substantiate identity), during increased FPCONS or Random Antiterrorism Measures (RAMs) include, but are not limited to:

3.7.8.1. School identification card with a photograph.

3.7.8.2. U.S. Military or draft record.

3.7.8.3. Native American Tribal Document.

3.7.8.4. U.S. Social Security card issued by the Social Security Administration (SSA).

3.7.8.5. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350).

3.7.8.6. U.S. Citizen ID Card (Form I-197).

3.7.8.7. ID Card for use of Resident Citizen in the United States (Form I-179).

3.7.8.8. Unexpired employment authorization document issued by the Department of Homeland Security (DHS), including (a) a Form I-94 identifying the holder as an asylee (by stating "asylum", "asylee" or appropriate provision of law), or (b) other documentation issued by DHS (or the former Immigration and Naturalization Service (INS)) that identifies the holder as an asylee, lawful permanent resident, refugee (except for the Form I-94 identifying the holder as a refugee, which is considered a receipt only), or other status authorized to work in the United States incident to status.

3.7.8.9. Foreign Military or Government Identification Credentials.

3.7.8.10. A foreign passport with a current Arrival-Departure Record (Form I-94) bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, if that status authorizes the alien to work for the employer.

3.7.8.11. In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement of the alien's nonimmigrant status, as long as the endorsement has not yet expired, and the proposed employment is not in conflict with any restrictions or limitations identified on the form.

3.7.9. To further support the identity proofing process, installations may use E-Verify to determine DHS-approved document authenticity, Social Security Number (SSN) verification, and SSA work authorization/visitor status when using these as ID proofing documents. E-

Verify (formerly the Basic Pilot/Employment Eligibility Verification Program) is an online system operated jointly by the DHS and the SSA and can be accessed via the following web address: http://www.dhs.gov/files/programs/gc_1185221678150.shtm. Participating employers can check the work status of new hires online by comparing information from an employee's I-9 form against SSA and DHS databases. E-Verify is free and voluntary, and is the best means available for determining employment eligibility of new hires and the validity of their Social Security numbers.

3.7.10. For OCONUS locations, Commanders will work with local and foreign authorities to identity proof applicants to the greatest extent practical and lawful.

3.7.11. In regions or locations with multiple installations, commanders may agree to reciprocally honor the identity proofing of other bases and Services. However, the need and fitness to access the installation must be determined at each installation. MAJCOMs will coordinate with Joint Commands at overseas locations to identify and implement credential efficiencies.

3.8. Approved Department of Defense (DoD) Privilege Card Holders.

3.8.1. DoDI 1330.21 and AFI 34-211(I) authorizes exchange privileges for certain credential holders (e.g., US Coast Guard Auxiliary), but these credentials are not authorized to facilitate unsponsored or unescorted entry to DoD installations.

3.8.2. Identity Proofing for this category of personnel is as follows:

3.8.2.1. In addition to providing an authorized document to validate their claim of authorization of limited exchange privileges as mandated in DoDI 1330.21 and AFI 34-211(I), these individuals will also be required to provide one other identity proofing document from section 3.7.6. to validate their identity.

3.8.2.2. Installations will codify access control procedures for this category of personnel in applicable access control plans.

3.9. Veterans Identification Card (VIC).

3.9.1. The Department of Veterans Affairs provides eligible Veterans a Veterans Identification Card (VIC) for use at Veterans Affairs (VA) Medical Facilities. Only Veterans who are eligible for VA medical benefits will receive the card. The card will only display the Veteran's name, picture, and special eligibility indicators (e.g. Service Connected, Purple Heart and Former Prisoner of War (POW)) on the front of the card, if applicable.

3.9.2. The VIC is only used for the purpose of identification and check-in for VA appointments, and does not by itself facilitate access to installations.

3.9.3. Identity Proofing for this category of personnel is as follows:

3.9.3.1. Eligible Veterans will provide the VIC at Installation Visitor Center's with VA Medical Facilities located on them to validate eligibility to receive a local pass/card. In addition to providing the VIC, these individuals will also be required to provide one other identity proofing document from section 3.7.6. to validate their identity.

3.9.3.2. Installations will codify identity proofing procedures for this category of personnel in applicable access control plans.

3.10. Outside the Continental United States (OCONUS).

3.10.1. OCONUS Installations will utilize appropriate ID proofing credentials such as a passport or nationally issued identity card or other IDs as approved by the COCOM.

3.10.2. OCONUS Installations will codify approved non-US ID proofing documents in local guidance.

3.11. Registration. All persons, who have demonstrated a need for an access credential and have had their identity proofed, will be registered in a local access control database.

3.11.1. Only personnel delegated by the installation commander shall perform access control authorizations and assignment of privileges. Delegation will be in writing, either by position designation codified in local guidance or name.

3.11.2. All biographic and biometric information gathered, stored, transmitted, and shared during registration, vetting, and screening will be considered controlled unclassified information (CUI) pursuant to Presidential Memorandum, *Controlled Unclassified Information*, and will minimize social security number use in accordance with USD(P&R) DTM 07-015, *DoD Social Security Number Reduction Plan*. This is based on the USAF's determination the CUI classification meets mission requirements, business prudence, the protection of personal rights, and safety/security. The National Archives and Records Administration (NARA) is the executive agent to oversee and implement the CUI framework. MAJCOMs and installations will, in their supplements to this instruction:

3.11.2.1. Determine the types of information to be collected within the standards of Chapters 2-3 of this AFI.

3.11.2.1. (ANG) Information to be collected will be predetermined by DBIDS or the electronic version of the AF Form 75. Access Control Logs may be utilized to supplement DBIDS or AF Form 75s, but will not contain any information in addition to that required by DBIDS or AF Form 75, unless determined mission essential by the local DFC.

3.11.2.2. Outline the purpose: To vet identity and security risk for access control (protection/law enforcement) as explained in Title 50, United States Code, Section 797, *Internal Security Act of 1950*.

3.11.2.3. Identify what information may be disclosed to whom during the access credential process and life of the access credential. Pursuant to references HSPD-6, *Integration and Use of Screening Information*, HSPD-11, *Comprehensive Terrorist-Related Screening Procedures*, and HSPD-24, *Biometrics for Identification and Screening to Enhance National Security*, disclosure/sharing can occur across the Federal government for the life of the issued access credential.

3.11.2.3. (ANG) Information contained within DBIDS, AF Form 75 or local Access Control Logs can only be disclosed/shared with military or civilian personnel assigned to or working with security forces units and personnel who are authorized to view Law Enforcement Sensitive data.

3.11.2.4. Outline how the information will be protected. All PII will be protected pursuant to the Privacy Act of 1974, DoD and USAF privacy programs.

FOR OFFICIAL USE ONLY

3.11.2.4. (ANG) All information obtained for or contained within DBIDS, AF Form 75s or local Access Control Logs will be protected under the Privacy Act of 1974, DoD and USAF privacy programs.

3.11.2.5. Identify the complete set of uses for the credential and related information. The uses will include identifying and responding to potential risks to DoD personnel, property, and national assets.

3.11.2.5. (ANG) DIBS and electronic AF Form 75s will only be used for access control to the local installation. Specific guidance for local installations will be contained within the installation's IDP.

3.11.2.6. (Added-ANG) The sponsor of visitor(s) identity must be verified prior to issuance of a visitor's pass. Telephone sponsorship is not authorized to include cases where caller ID exists. Sponsors will make physical contact with the visitor center or gate to verify their identity when sponsoring visitors. *EXCEPTION:* Installations may use digitally signed emails from DoD accounts as a verification of sponsorship identity with approval from the local IDC. If utilized, this procedure will be identified in the IDC Minutes and incorporated into the next revision of the IDP.

3.12. Unique Considerations/Special Events/Exceptions to Policy.

3.12.1. For unique circumstances requiring one-time access, the USAF authorizes installations to use other mechanisms to grant visitors installation access. For these events, unescorted/uncontrolled access will only be granted for individuals who have been appropriately identity proofed and vetted.

3.12.2. If an event's population size makes this practice prohibitive (large functions such as graduations, air shows, sporting events, concerts, etc.), the installation will employ compensatory security measures to control circulation of un-proofed or un-vetted populations. Those personnel who have not been identity proofed or vetted will not have unescorted, uncontrolled physical access to and within installations. For further details, please refer to AFI 10-1004, *Conducting Air Force Open Houses*.

3.12.3. (Added-ANG) Installation commanders should consider added compensatory measures for unique circumstances/special events to include random vehicle inspections on a percentage of vehicles entering for purpose of special event as determined by the installation commander.

Chapter 4

IDENTITY VETTING AND FITNESS DETERMINATION

4.1. Identity Vetting Concept. Once an individual has undergone successful identity proofing pursuant to Chapter 3, Installation Commanders must determine the individual's fitness for installation entry: namely, the local determination whether an individual poses an unreasonable threat to USAF resources or personnel if granted installation access. This chapter outlines the means for determining fitness through the vetting of proofed identities. **Note:** Only personnel delegated by the installation commander in writing shall perform vetting. Delegation will be in writing, either by position designation codified in local guidance or name.

4.2. Common Access Card (CAC) Populations. Identity vetting requirements for CAC populations is prescribed in AFI 36-3026 (IP), Volume 1; HSPD-12; DTM 09-012; and OMB implementing guidance and instructions. **Note:** The vetting requirement for Active Duty, Civilian Employee and Contractor Eligible CAC holder personnel includes a minimum NACI or equivalent investigations. Fitness standards for these populations are listed in AFI 31-501, *Personnel Security Program Management*.

4.3. Non-Common Access Card (CAC) Department of Defense (DoD) Populations. Identity vetting requirements for military, retiree/dependent, civilian (included non-appropriated) and contractor populations is prescribed in AFI 36-3026 (IP), Volume 1; DTM 09-012; and Office of Management and Budget implementing guidance and instructions.

4.3.1. The vetting requirement for Active Duty, Civilian Employee and Contractor Eligible Non-CAC DoD credential holders includes a minimum NACI or equivalent investigations. Fitness standards for these populations are listed in AFI 31-501.

4.3.2. Retiree personnel had their NACI or equivalent investigation while on active duty.

4.3.3. The dependent population has not been properly vetted. However, their approved DoD sponsor assumes responsibility for assuring their fitness is appropriate to enter an Air Force Installation.

4.4. Non-Department of Defense (DoD) Federal Personal Identity Verification (PIV) Populations. Per DTM 09-012, personnel in possession of a valid Federal PIV are considered identity proofed and vetted for the purpose of installation access. However, these individuals are not allowed unabated access without sponsorship or a valid need for entry as determined by Installation Commander.

4.5. Transportation Worker Identification Credential (TWIC) Holders. Per DoD policy, personnel in possession of a valid TWIC are considered identity proofed and vetted for the purpose of installation access. However, these individuals are not allowed unabated access without sponsorship or a valid need for entry as determined by Installation Commander.

4.6. Personal Identity Verification-Interoperable (PIV-I) Credentials. PIV-I credentials require vetting via a NCIC basic name check (please see section 5.2.1.2. for information on an NCIC Name Check) and TSDB (when available) to be allowed unescorted access to an installation. However, these individuals are not allowed unabated access without sponsorship and a valid need for entry as determined by Installation Commander.

FOR OFFICIAL USE ONLY

4.7. Locally Produced Physical Access Control System (PACS) Passes/Cards and AF Form 75 Visitor Pass/Vehicle Pass. With the need for access and successful identity proofing complete, the USAF will ensure vetting of proofed identities for other populations that do not possess a credential authorized to facilitate access to determine fitness for access or whether potential access candidates pose a potential threat or risk to installations, resources, and populations.

4.7.1. The vetting standard for physical access and generation of access credentials include querying the government databases listed in this section, as available and within the law. Installations will vet access candidates to the greatest extent practicable and lawful.

4.7.2. All personnel requiring unescorted access to installations that do not possess a credential authorized to facilitate access must be vetted against government authoritative databases.

4.7.3. At a minimum, installations will determine fitness of individuals through NCIC (via a name check) and TSDB (when available). In addition to connections through State terminals, a web-based application is available through the Department of Justice which allows CONUS and OCONUS installations to access NCIC (with Interpol links) without using State systems.

4.7.3. (ANG) An NCIC Originating Agency Identifier (ORI) is a nine-character identifier assigned by the FBI NCIC to an agency which has met the established qualifying criteria for an ORI assignment to identify the agency in NCIC and NLETS transactions. NGB/A7SO maintains a listing of NCIC ORIs for assigned Security Forces units. Presentation of NCIC ORI numbers to officials granting access to NCIC systems should resolve access authority conflicts.

4.7.3.1. For OCONUS locations, Commanders will work with local and foreign authorities to vet applicants to the greatest extent practical and lawful.

4.7.3.2. At OCONUS locations, installations may deviate from the requirements where local conditions, treaties, agreements, and other foreign governments and allied forces require different standards. **Note:** In these cases, MAJCOMs and installations will determine the fitness and eligibility for an individual to access their installations and will work with local and foreign governments to vet applicants.

4.7.3.3. In foreign countries, local embassies and host nation law enforcement agencies may support access control decisions with identifying vetting of potential access candidates.

4.7.4. Strongly recommend authorized personnel performing the vetting process be armed in case a dangerous individual is identified during screening. If personnel cannot be armed, a covert, duress alarm which annunciates in BDOC is required.

4.7.5. Installations Commanders can also direct queries to other government authoritative databases. These include, but are not limited to:

4.7.5.1. DoD's Automated Biometrics Identification System (ABIS).

4.7.5.2. The Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS).

4.7.5.3. Department of Homeland Security (E-Verify).

4.7.5.4. Department of Homeland Security (U.S. VISIT).

4.7.5.5. Department of State Consular Checks (non U.S. citizen).

4.7.6. Any additional data sources queried that are not listed will be approved by the servicing legal office.

4.8. Approved DoD Privilege Card Holders.

4.8.1. DoDI 1330.21 and AFI 34-211(I) authorizes exchange privileges for certain credential holders (e.g., US Coast Guard Auxiliary), but these credentials are not authorized to facilitate unsponsored or unescorted entry to DoD installations.

4.8.2. With the exception of US Coast Guard Auxiliary personnel who possess a Coast Guard Auxiliary ID Card CG-2650, all other personnel authorized limited exchange privileges who do not possess an authorized credential to facilitate access that is considered properly vetted per this instruction will be vetted against government authoritative databases as mandated in this chapter.

4.9. Veterans Identification Card (VIC).

4.9.1. The Department of Veterans Affairs provides eligible Veterans a Veterans Identification Card (VIC) for use at Veterans Affairs (VA) Medical Facilities. Only Veterans who are eligible for VA medical benefits will receive the card. The card will only display the Veteran's name, picture, and special eligibility indicators (e.g. Service Connected, Purple Heart and Former Prisoner of War (POW)) on the front of the card, if applicable.

4.9.2. The VIC is only used for the purpose of identification and check-in for VA appointments, and does not by itself facilitate access to installations.

4.9.3. Eligible Veterans will provide the VIC at Installation Visitor Center's with VA Medical Facilities located on them to validate eligibility to receive a local pass/card. In addition to providing the VIC, these individuals will also be required to provide one other identity proofing document from section 3.7.6. to validate their identity.

4.9.4. VIC holders who do not possess an authorized credential to facilitate access that is considered properly vetted per this instruction will be vetted against government authoritative databases as mandated in this chapter.

4.10. Foreign Visitors. For officially-sponsored visits of foreign military members and their families to CONUS installations, MAJCOMs, installations, and units will use FVS and FVS-CM to verify the vetting of these populations pursuant to DoDD 5230.20, AFI 16-107, AFI 16-201, and AFD 16-1.

4.11. Housing Privatization Personnel. The Access Integrity Unit of the FBI's Office of General Counsel has determined civilians applying for residence in privatized housing on military installations fall within the scope of previous authorizations for using the NCIC (via a name check) and the Interstate Identification Index (III) on visitors to military installations.

4.11.1. As a result, installations are authorized to conduct name-only background checks (name check) on those applying for housing on a military installation and current individuals

already residing in housing on military installations who have not already been subject to a background check. Please see section 5.2.1.2. for information on an NCIC Name Check.

4.11.2. As privatized housing residents are considered "visitors" once, name checks may not be regularly performed for site security purposes. However, subsequent name checks may be authorized if there is reasonable suspicion/probable cause to suspect criminal activity. Installations will consult with their servicing Staff Judge Advocate (SJA) when making these decisions.

4.11.3. The following vetting standards apply to Housing Privatization Personnel based on their category:

4.11.3.1. Category 1 – Project Owner Corporate/Regional Personnel (sponsored by AFCEE/HP). Category 1 personnel are issued a CAC and are required to have a NACI or equivalent investigation/adjudication.

4.11.3.2. Category 2 – Project Owner Property Management/Maintenance Personnel (sponsored by the Base's Capital Asset Manager). Category 2 personnel are issued a local credential and are required to have an NCIC name check completed. Please see section 5.2.1.2. for information on an NCIC name check.

4.11.3.3. Category 3 – Project Owner Contractors/Subcontractors (sponsored by the Base's Capital Asset Manager). Category 3 personnel are issued a local credential and are required to have an NCIC name check completed. Please see section 5.2.1.2. for information on an NCIC name check.

4.11.3.4. Category 4 – Eligible Tenants/Housing Occupants (sponsored by the Base's Capital Asset Manager). Category 4 personnel are issued a local credential and are required to have an NCIC name check completed. Please see section 5.2.1.2. for information on an NCIC name check.

4.12. Non-authoritative Databases. Currently, systems are employed in the USAF which do not connect to government authoritative databases and mine potentially discriminating data from open-sources.

4.12.1. These systems must meet the specifications of USAF privacy standards, be accredited and certified to operate on the USAF GIG, and have at least an Interim Authority to Operate authorization.

4.12.2. Installations may continue to use these systems within formal DoD and USAF specifications, but the systems will not be used as the sole source for determining fitness for access.

4.12.3. All information gleaned from these open source systems must be verified with authoritative government sources before access decisions are approved or denied.

4.13. Fitness Determination. Specific guidance for denial of installation access will be included in local instructions.

4.13.1. Only personnel delegated by the installation commander in writing shall perform fitness determination. Delegation will be in writing, either by position designation codified in local guidance or name.

4.13.2. Installation Commanders may deny access and access credentials based on information obtained during identity vetting that indicates the individual may present a threat to the good order, discipline and morale of the installation, including, but not limited to the following:

4.13.2.1. The individual is known to be or reasonably suspected of being a terrorist or belongs to an organization with known terrorism links/support.

4.13.2.2. The installation is unable to verify the individual's claimed identity.

4.13.2.3. There is a reasonable basis to believe the individual has submitted fraudulent information concerning his or her identity.

4.13.2.4. There is a reasonable basis to believe the individual will attempt to gain unauthorized access to classified documents, information protected by the Privacy Act, information that is proprietary in nature, or other sensitive or protected information.

4.13.2.5. There is a reasonable basis to believe the individual will unlawfully or inappropriately use an access credential outside the workplace.

4.13.2.6. There is a reasonable basis to believe, based on an individual's criminal or dishonest history, that issuance of an access credential poses an unacceptable risk to the installation/mission.

4.13.2.7. The individual has/had been barred from entry/access to a Federal installation or facility.

4.13.2.8. The individual is wanted by Federal or civil law enforcement authorities, regardless of offense or violation.

4.13.2.9. The individual has been incarcerated within the past ten years, regardless of offense/violation, unless released on proof of innocence.

4.13.2.10. The individual has any conviction for espionage, sabotage, treason, terrorism, or murder.

4.13.2.11. The individual's name appears on any Federal or State agency's "watch list" or "hit list" for criminal behavior or terrorist activity.

4.13.2.12. The individual has been convicted of a firearms or explosive violation within the past ten years.

4.13.2.13. The individual has been convicted of sexual assault, armed robbery, rape, child molestation, child pornography, trafficking in humans, drug possession with intent to sell or drug distribution.

4.13.2.14. There is a reasonable basis to believe, based on the individual's material, intentional false statement, deception, or fraud in connection with Federal or contract employment, that issuance of an access credential poses an unacceptable risk to the installation/mission.

4.13.2.15. There is a reasonable basis to believe, based on the nature or duration of the individual's alcohol abuse without evidence of substantial rehabilitation, that issuance of an access credential poses an unacceptable risk to the installation/mission.

FOR OFFICIAL USE ONLY

4.13.2.16. There is a reasonable basis to believe, based on the nature or duration of the individual's illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation, that issuance of an access credential poses an unacceptable risk to the installation/mission.

4.13.2.17. A statutory or regulatory bar prevents the individual's contract employment; or would prevent Federal employment under circumstances that furnish a reasonable basis to believe that issuance of an access credential poses an unacceptable risk to the installation/mission.

4.13.2.18. The individual has knowingly and willfully engaged in acts or activities designed to overthrow the U.S. Government by force.

4.14. Debarment. AFI 31-101 and AFMAN 31-201V7, *Security Forces Administration and Reports*, provides guidance on debarments.

4.14.1. An Installation Commander may deny an individual access for involvement in the commission of a criminal offense, when access is inconsistent with the interests of national security, when personal conduct reflects negatively on the image of the US overseas, or when access adversely affects the health, safety, or morale of personnel on that installation.

4.14.1.1. Subject to any host-nation agreement, Installation Commanders may deny access to the installation through the use of a debarment order.

4.14.1.1.1. Installation Commanders may not delegate this authority.

4.14.1.1.2. Debarment letters will be coordinated through the servicing legal office.

4.14.1.1.3. Documentation supporting debarment must be kept for the period of the debarment.

4.14.1.1.4. Anyone debarred from an installation may petition the Installation Commander for partial or limited privileges.

4.14.1.2. A commander's decision to debar must be based upon investigative evidence, documented facts, and the written coordination of the servicing judge advocate's office or legal representative when deciding if an incident is serious enough to warrant a debarment.

4.14.1.3. Coordination and other documentation leading to the debarment decision will be maintained as a part of the official debarment file and must be kept for the period of the debarment.

4.14.1.4. To restrict access to installation facilities (e.g., commissary, post exchange, and class VI), commanders may consider alternatives to an installation debarment.

4.14.1.5. Actions against civilian employees will also be coordinated through the servicing personnel office. Such coordination will be made a part of the official file.

4.14.1.6. Actions to debar contractors from access to installations will be coordinated with the local contracting office.

4.14.1.7. On rare occasions, Installation Commanders may impose limited debarments on individuals that do not restrict access under certain circumstances, such as allowing access to places of duty.

- 4.14.1.7.1. In these situations, the commander must concurrently consider revoking the individual's vehicle registration privileges and driving privileges.
- 4.14.1.7.2. In cases of total debarment, vehicle registration rights are automatically revoked, but failure to specify this action for a limited debarment will require the commander to make a determination each time the individual registers the vehicle.
- 4.14.2. Debarment Orders. Debarment orders should be in writing and contain sufficient details to support prosecution by civilian authorities.
 - 4.14.2.1. The debarment order must also state the period of debarment or permanent debarment.
 - 4.14.2.2. See AFMAN 31-201 Volume 7 for an outline when preparing debarment orders.
 - 4.14.2.3. If practical, debarment letters should be hand-delivered. If hand delivery is impractical, debarment letters should be sent by certified mail to ensure a record of receipt.
 - 4.14.2.4. Oral debarment orders should be given only when time constraints prevent preparing a written order, or the severity of the crime warrants immediate debarment.
 - 4.14.2.4.1. Oral debarments must be documented in the SF blotter with the time, date and name of the commander giving the order.
 - 4.14.2.4.2. In all cases, oral debarments must be immediately followed-up in writing within 24-hours or the next duty day.
 - 4.14.2.5. Debarments to be implemented from other installations should be initiated by the SF Reports and Analysis Section upon receipt of the documentation from the installation issuing the debarment order.
 - 4.14.2.6. Installations will enter debarment information into SFMIS.
 - 4.14.2.6.1. PACS will have the capability to display debarment status on registered individuals.
 - 4.14.2.6.2. In cases where a debarred individual is flagged at another base using a PACS, each Installation Commander will be informed of the debarment to consider whether or not he/she will also debar the individual at his/her installation.
- 4.14.3. Security Forces will maintain a list of personnel debarred from the installation. All lists are FOUO.
 - 4.14.3.1. Use local procedures to update the list. Do not release lists to the public, leave them unsecured or place them where unauthorized personnel can view them.
 - 4.14.3.2. Debarment lists may be combined and maintained in the same manner as lists used for tracking and documenting personnel denied on-base driving or other privileges.
- 4.14.4. Disposition.
 - 4.14.4.1. Installation Commanders will designate the period of debarment or permanent debarment, except during cases of emergency as specified, for example, in 4.14.5.5.3.

FOR OFFICIAL USE ONLY

4.14.4.2. Installation Commanders, after consulting with the servicing judge advocate's office or legal representative, will determine the length of debarment or permanent debarment.

4.14.4.3. Once imposed, Installation Commanders will ensure that the debarment information is provided to the appropriate SF unit for registration into interoperable Joint databases (if applicable) and SFMIS.

4.14.4.4. One copy of the debarment action, along with all supporting enclosures, will be maintained by the security forces squadron.

4.14.5. Legal Entitlement.

4.14.5.1. For purposes of section 4.14.5, "active duty members" include reserve military personnel on active duty and assigned for duty to USAF installations; and "civilian employees" which include both US (appropriated and non- appropriated fund, to include US invited contractor employees) and HN (appropriated and non-appropriated, to include US invited contractor employees).

4.14.5.2. Subject to the provisions below, active duty members, dependent family members and retirees may not be completely debarred from the installation or facility to which they are assigned, employed, or are required to enter on official job-related or benefits related business. Examples include military members and their dependents, who are eligible for military medical care and cannot be turned away (legislative in nature). Installations will work with their servicing legal office to determine if other reasonable access to appropriate medical care exists. All other personnel may be debarred from an installation or facility as necessary.

4.14.5.3. If individuals with legal rights are debarred from installations or facilities, specific provisions for limited access for the continued exercise of these legal rights must be offered and explained in detail within the debarment letter. Some examples of these provisions include a required single entry and exit point at the installation, requirement of prior notice to the Installation Commander for official escort, etc. Installations will codify procedures in local guidance for allowing debarred personnel with limited access onto and off the installation.

4.14.5.4. Access to areas within an installation or facility may be limited or restricted where no employment-related access needs exist.

4.14.5.5. Military members pending discharge from the Armed Forces may be debarred from their former place of duty and/or other locations on a USAF installation if their presence in such locations would interfere with the mission or would be prejudicial to good order and discipline.

4.14.5.5.1. If the debarment authority determines that, based on the nature of the misconduct, a civilian employee is a serious threat to the health, safety, or security of the installation or facility, (e.g., bringing a weapon onto the installation, stealing classified documents, threatening bodily harm or destruction of government property) the employee's sponsoring unit and immediate supervisor will be contacted to place the employee on enforced leave with intent to take removal action.

4.14.5.5.2. After the employee is placed on enforced leave, the Installation Commander may completely debar the individual from the installation or facility.

4.14.5.5.3. If an Installation Commander, in a very unusual case, determines that a civilian employee poses a serious and imminent threat to the health, safety, or security of the installation or facility, he/she may take immediate action.

4.14.5.5.3.1. This action may include a temporary debarment to remove the employee from the installation or facility.

4.14.5.5.3.2. In such cases, the debarment authority will coordinate with the servicing civilian personnel advisory center or Civilian Personnel Elements and the employee's supervisory chain as soon as practical thereafter for a permanent and/or complete debarment of the employee, if necessary.

4.14.6. Debarment Rosters. Security personnel at local Pass and Registration Offices, Base Defense Operations Centers (BDOC), installation access control points, and visitor centers will use the PACS (if applicable) or local debarment roster to ensure that unauthorized personnel are not allowed access, and if applicable, charged with trespassing when entry is illegally gained.

4.14.7. Reinstatement.

4.14.7.1. Any debarred person may request reinstatement as indicated in the debarment letter.

4.14.7.2. If requested by the debarred individual, debarment actions can be reviewed by the Installation Commander for possible removal of the debarment and reinstatement of access privileges.

4.14.7.3. The Installation Commander is the final authority for removal or reinstating debarment actions.

4.14.7.4. If the Installation Commander decides to remove the debarment, the affected person and other agencies previously informed of the debarment action will be provided a copy of the letter removing the debarment (in English and HN language as applicable).

4.14.8. Appeal Process.

4.14.8.1. Commanders empowered to impose debarment actions have the authority and latitude to establish procedures concerning locally imposed debarment actions and appeal processes for those debarment actions.

4.14.8.2. Any and/or all appeal processes will be stated in the debarment letter.

4.14.8.3. See paragraph 4.14.7. regarding relief provisions from debarment actions.

4.14.8.4. Individuals may submit matters of reconsideration to the imposing commander, who may reevaluate the debarment, especially in instances of administrative error or mistaken identity. If the installation has established appeals processes, individuals seeking reconsideration must submit matters IAW those processes.

4.14.8.5. Per approved policy, the United States Forces Japan (USFJ)-wide and United States Forces Korea (USFK)-wide installation and area level debarments are not subject to appeal unless specifically allowed by the imposing commander.

FOR OFFICIAL USE ONLY

Chapter 5

PERIODIC SCREENING REQUIREMENTS OVERVIEW

5.1. Inherent Vulnerability. Access credentials are based on the initially successful determination of access need, identity proofing, and vetting process to determine fitness for entry.

5.1.1. Once any access credential is issued, fitness is not normally determined again until the credential expires, and a new one is issued. In some cases, the time between credential issuance and expiration could be lengthy. Therefore, a person's fitness for entry may change at any point prior to expiration without the knowledge of the Installation Commander (felony wants/warrants, terrorist nexus, or other potential disqualifiers).

5.1.2. Current system interoperability and connectivity does not allow for automatic updates from "authoritative" government databases to local access systems. An Identity Management Enterprise Services Architecture is being developed that will enable PACS to receive continuous information management updates from "authoritative" databases on all authorized credentials to validate an individual's fitness and authorization to enter an installation. Information on the Identity Management Enterprise Services Architecture is contained in Chapter 7.

5.2. Procedures.

5.2.1. NCIC. Per current mandates, Installations Commanders are only currently authorized:

5.2.1.1. To conduct a name check per visit, or if someone is visiting for multiple days, a name check each time they come to the gate, on non-DoD affiliated civilian visitors; excluding privatized housing residents per Section 4.11.2., as privatized housing residents are considered "visitors" once, thus name checks may not be regularly performed for site security purposes.

5.2.1.2. NCIC Name Check: Name check refers to the type of NCIC check conducted, it does not mean the NCIC operator is only allowed to enter the person's name they are running the check on. NCIC name checks field include, but are not limited to a person's name, sex, race, date of birth and social security number.

5.2.2. The last date of periodic screening will be listed in the database (PACS or locally developed procedures until PACS are installed) used to track installation visitors.

5.2.3. If disqualifying information is revealed on a person who has already been issued a temporary access credential, the Installation Commander will determine whether continued unescorted access will be granted based on the new information. Until this determination is made, the person's unescorted access to the installation must be denied.

5.2.3.1. If the Installation Commander determines access will no longer be granted, SF will promptly update the local database with the decision date and will notify the sponsor and the credential holder of the action and reason for access termination.

5.2.3.2. Personnel who have been denied access after issuance of an access credential may appeal such denial through the Installation Commander or his designated representative and the servicing judge advocate's office or legal representative.

FOR OFFICIAL USE ONLY

5.2.3.3. If the Installation Commander determines access will continue to be granted, SF will promptly update the local database with the decision date and will notify the sponsor and the credential holder of the action and reason for continued access.

5.2.4. Once the temporary credential expires, the person's fitness for installation access will be fully vetted again.

Chapter 6

INSTALLATION PERIMETER ENTRY CONTROL POINT OPERATIONS

6.1. United States Air Force (USAF) Installation Perimeter Access Control Guidance. This chapter establishes USAF policy on installation perimeter entry control points and controlling access. Additional measures and TTPs may be found in AFTTP 3-31.1, *Entry Control*. The following minimum standards may be supplemented by the MAJCOM or installation based on the type of installation involved, assets/facilities located on the installation, types of individuals requiring entry, or other exigent circumstances.

6.1.1. Installation access will be controlled at all USAF installation perimeters by channeling all vehicles and personnel to designated entry control points while maximizing, to the greatest extent practical based on local threat assessments and the Installation Commander's risk assumption, the ability to prevent and detect unauthorized entry at other points along the base perimeter. **Note:** Installation Commanders will determine perimeter access control procedures for off-base government housing areas.

6.1.2. Installations will include access control in their published integrated defense or security plans as this Law and Order function is an integral aspect of base defense.

6.1.3. Installation Commanders will coordinate and seek to standardize and integrate access control procedures and local credentials with other military installations in their area.

6.2. Construction Standards.

6.2.1. Except as otherwise allowed by a properly approved waiver or exemption, USAF installations will meet applicable physical security standards for installation perimeters in accordance with AFI 31-101 and UFC 4-022-01. USAF Installations will also ensure coordination with the Airfield Manager and airfield design office to mitigate risks to flight and ground safety in accordance with UFC 3-260-01, *Airport and Heliport Planning and Design*, and UFC 3-535-01, *Visual Air Navigation Facilities*.

6.2.2. Construction Standards. Effective installation entry control point and visitor center design requires the integration of the civil engineering, communications, and physical security disciplines. New and modified facilities will comply, as applicable, with UFC 4-022-01.

6.2.3. Installation perimeter access control includes elements of engineering (gate construction and design), physical security equipment (lighting, cameras, sensors, barriers/bollards/speed mitigation devices, channeling tools, signs, ballistic protection, network access, credential/biometric readers), and communications (computers, networks, databases, radios). Therefore, any successful effort to design or improve installation access control must include the expertise of and coordination among many base agencies and consider the following factors:

6.2.3.1. Criticality of assets located within the installation perimeter.

6.2.3.2. Local threats to installation facilities, population, and assets.

6.2.3.3. Current base access vulnerabilities and capability gaps to include perimeter barriers, lighting, signage, networks, wireless networks/connections and communications

FOR OFFICIAL USE ONLY

as well as the ability of personnel to enter the base perimeter undetected or via a forged, counterfeit, or fraudulent access credential or identity source document.

6.2.3.4. The cost or technological feasibility/availability of correcting vulnerabilities when compared to the threat (risk assumption).

6.2.3.5. Base population size and throughput requirements.

6.2.3.6. Access population groups (active duty military, retirees, dependents, contractors, vendors, foreign official visitors, tenant organizations, etc.).

6.2.3.7. Proximity to other joint, USAF or sister Service installations.

6.2.3.8. Integration with other defense in depth measures and forces.

6.2.3.9. Communication and teaming with local authorities and first responders.

6.2.3.10. Force protection policies and requirements of the owning Combatant Commander.

6.2.3.11. Installation Commander's risk tolerance.

6.2.4. Installations should plan for the development of Visitor Centers, adjacent to and external to an installation entry control point, as applicable. Processing visitors outside the installation or at the perimeter prevents unnecessary access for potential threats to USAF personnel or resources.

6.2.4. (ANG) Most ANG installations do not have enough visitors to warrant the expense, the geographical space to build, or the manpower to cover the additional posting associated with a Visitor's Center. Commanders should carefully weigh the benefits in comparison to the associated costs when making a determination on the necessity of a Visitor's Center.

6.2.4.1. Visitor Centers will have access to the USAF GIG, SFMIS, and authoritative government databases to greatest extent practicable and will be operated by authorized, trained and certified personnel. These requirements expedite the processing of visitors to the installation to include fitness determination.

6.2.4.2. Installation Commanders will determine hours of operation for Visitor's Centers and will exercise prudence when displaying or distributing materials at Visitor's Centers which provide unnecessary information to individuals who have not been processed for entry.

6.3. Installation Perimeter Access Control Measures.

6.3.1. Armed and trained USAF Security Forces personnel, armed Department of the Air Force (DAF) civilian police/guards or armed contract guards will control entry to USAF installations. A minimum of two personnel will secure each manned entry control point when in operation; one may operate as an over watch. These personnel may be augmented, at the Installation Commander's discretion, by trained non-SF personnel based on mission needs or emergency circumstances.

6.3.2. A minimum of two personnel familiarized on visitor center procedures will be posted at the Visitor Center at all times, when the Visitor Center is in operation. One person may issue PACS passes/cards, provide directions to visitors, etc; and one person may conduct the identity proofing and vetting requirements mandated in DTM 09-012. **Note:** As mentioned

FOR OFFICIAL USE ONLY

in section 4.7.4., it is strongly recommended personnel performing the vetting process be armed in case a dangerous individual is identified during screening. If personnel cannot be armed, a covert, duress alarm which annunciates in BDOC is required.

6.3.3. A minimum of three armed USAF Security Forces personnel, armed DAF civilian police/guards or armed contract guards personnel will be posted at each Commercial Vehicle Search area at all times when in operation.

6.3.4. Entry control point personnel will be positioned in a manner to safely monitor inbound and outbound pedestrian and vehicle traffic, operate barrier systems and equipment as applicable, and detect potential threats as far from their position as possible.

6.3.5. Installations will emplace speed calming devices to create a serpentine effect on inbound and out-bound lanes at perimeter ECPs to mitigate high-speed approaches and to inhibit base entry through exit lanes.

6.3.6. FPCON signs and applicable special instructions will be posted to properly inform vehicles and pedestrians as they approach the entry control point.

6.3.7. Installations will ensure that all first-time arrivals and final departures of official foreign visitors will be recorded using the FVS-CM pursuant to DoDD 5230.20, AFI 16-107, AFI 16-201, and AFD 16-1, when determining sponsorship and affiliation and issuing access credentials. **Note:** It is the sponsoring organization's responsibility to ensure the visit is properly recorded and documented in the DoD FVS; and the local AFOSI unit is notified when official foreign visitors arrive and depart the installation.

6.3.8. All POVs accessing the installation must be properly licensed, inspected, and insured in accordance with Combatant Command, state, local and host nation laws, as applicable.

6.3.8.1. Rental vehicles are considered POVs for the purpose of base entry and access control. All vehicles rented or leased by AFOSI, FBI, and USSS for official duties are considered government vehicles and qualify as "official vehicles" at 6.3.10.

6.3.8.2. SF will monitor and enforce these requirements when issuing temporary credentials, during Random Installation Entry/Exit Vehicle Checks (RIEVC), other random vehicle searches or as dictated in higher FPCONs.

6.3.9. Commercial, delivery, and/or contract vehicles providing authorized services to installation customers may enter AF installations unescorted after authorized installation personnel have verified a valid need for entry and the driver and passenger(s) who do not already have an approved access credential have been identity proofed and received a favorable check/vetting from authoritative government databases. Examples include, but are not limited to, moving vans, furniture delivery vehicles and taxi services.

6.3.9.1. SF will conduct a 100% search/sweep for explosives and contraband on all large commercial, delivery, and/or contract vehicles entering USAF installations using MWD teams and/or commercial explosive detection equipment, if available, using Air Force Handbook (AFH) 10-2401, *Vehicle Bomb Mitigation Guide*, as a reference. Using MAJCOM guidance, local planners will define in integrated defense plans what type of vehicles fit in the definition of a large vehicle based on their geographic location, character of local transport and threat. The following guidelines should be followed when conducting vehicle searches:

FOR OFFICIAL USE ONLY

6.3.9.1. (ANG) Local planners will define in integrated defense plans what type of vehicles fit in the definition of large vehicle based on their geographic location, character of local transport and threat. However, the definition of a large vehicle will normally encompass a non-government or non-privately owned vehicle weighing 10,000 lbs or more.

6.3.9.1.1. Ensure the engine is off and the parking brake is set when inspecting a vehicle.

6.3.9.1.2. Use the team approach to inspecting (i.e., inspection team overwatch).

6.3.9.1.3. Know where the driver and passengers are at all times.

6.3.9.1.4. The driver shall open all doors, hood, trunk, compartments, etc., and every time the vehicle enters the search area, searchers shall conduct a thorough inspection. Ensure no areas are missed.

6.3.9.1.5. Do not allow vehicle occupants to be present if the searchers feel their safety is endangered. Have the occupants escorted to a safe area.

6.3.9.1.6. Ensure searchers inspect vehicle documentation. Examples of documentation to be inspected (as applicable) include vehicle registration, gas receipts, driver's license, logbook, manifest, shipping papers (bill of lading) and itinerary.

6.3.9.1.7. Ensure commercial vehicles are properly displaying vehicle markings.

6.3.9.1.8. After the vehicle has completed the inspection and has been determined to be safe to enter the installation, non-ID card holders will then be provided a pass.

6.3.10. SF will conduct RIEVCs. However, on duty AFOSI personnel and Federal, State, Local and Tribal law enforcement personnel in official vehicles will be exempt from random vehicle inspections if it interferes with an investigation or official government business.

6.3.11. Substantiated and approved munitions shipments, due to their sensitive nature, will not be diverted except in emergencies. Transportation Management Office personnel will escort scheduled munitions shipments from base access points to suspect and cargo hold areas pending final disposition.

6.3.12. Access control measures for Unique Circumstances/Special Events.

6.3.12.1. Installation Commanders may use other measures including, but not limited to, entry access lists or access memoranda for specific special events or unique circumstances.

6.3.12.1.1. In these cases, driver's licenses, passports, or other means of photo identification may be used in concert with the entry access list for access.

6.3.12.1.2. Names on these documents should be vetted against authoritative government databases as specified in this instruction for potential derogatory fitness information.

6.3.12.2. The USAF encourages commanders to minimize the use of these measures and use PACS passes/cards, AF Forms 75s, or other credentials, when applicable.

FOR OFFICIAL USE ONLY

6.3.12.3. For initial access of official foreign visitors or others who require the eventual issuance of a CAC, an Entry Authority List (EAL), AF Form 75, or PACS pass/card may be used following access need determination/sponsorship, identity proofing and vetting.

Note: For these situations, installations will employ compensatory measures to ensure circulation control and protection of resources.

6.3.13. Integrated Defense Risk Management Process (IDRMP). IDRMP is used to determine how best to use limited personnel and resources to protect personnel and assets. The IDRMP provides a more precise understanding of how the three risk factors of threat, vulnerability and asset criticality relate to each other at each installation. Installation Commanders may use the IDRMP process for access control. Please refer to AFI 31-101 for more information.

6.3.14. Installations should vary access control procedures to avoid predictability to adversaries gathering information for the purpose of unauthorized entry.

6.4. Installation Perimeter Access Control Minimum Standards for Controlling Physical Access.

6.4.1. The minimum USAF standard for controlling physical access to an installation via a manned entry control point, when funding becomes available, shall be:

6.4.1.1. An electronic PACS that provides the capability to rapidly and electronically authenticate credentials and individual authorization and fitness to enter an installation. Installations must also purchase an approved pass/card issuance systems to be used in conjunction with PACS.

6.4.1.1. (ANG) The chosen PAQS for ANG bases is DBIDS.

6.4.1.1.1. To ensure effective use of resources, long-term sustainability and DoD/Federal wide interoperability, installations will coordinate all installation and internal access control system and component purchases with MAJCOM A7S Divisions and the HQ AFSFC/SFXR (Requirements Branch) prior to funding obligation and execution.

6.4.1.1.1. (ANG) The POC for procurement of PACS within ANG is NGB/A7SX.

6.4.1.1.2. Any PACS which connect to the USAF GIG must be accredited and certified in concert with local and USAF communications entities and complete a thorough PIA.

6.4.1.2. PACS must support a DoD-wide and Federally interoperable access control capability that can authenticate United States Government physical access credentials and support access enrollment, authorization processes, and secure information sharing.

6.4.1.3. The electronic interrogation will include verifying the validity of the credential and matching the identity of the individual to a registered account within an access control database which stores privileges, prohibitions, and restrictions for access.

6.4.1.4. Biometrics may be added to the PACS when infrastructure, capability, resources are available and as legal issues regarding their use, storage, transmission and retention are resolved. Please see Chapter 8 for more information on biometrics.

6.4.1.5. At bases with PACS installed and operational, registration is mandatory. Although PACS are designed to ensure 100 percent accountability of personnel accessing USAF installations, there may be situations when the use of the system is not feasible or appropriate. Each installation will determine the specific utilization to meet their operational needs outside of the minimum parameters of this instruction.

6.4.2. Where PACS are not installed, the minimum USAF standard for controlling physical access to an installation via a manned entry control point shall be a physical and visual inspection of credentials by installation entry controllers at perimeter physical entry and/or access control points. The visual/physical inspection of the credential will include:

6.4.2.1. A verification of the authenticity of the credential.

6.4.2.1.1. The protective measures built into credentials may include, but are not limited to, holograms, micro-printing, watermarks, or local authenticators (e.g., IR stamp, number authenticators, etc.).

6.4.2.1.2. The CAC's protective measures include the watermark and hologram. Retired and dependent credentials include holograms.

6.4.2.2. A visual match of the photograph of the person presenting the identification.

6.4.2.3. A check of the expiration date of the credential.

6.4.2.4. A check of any date/time restrictions on the credential.

6.4.3. Once the credential is validated and the individual's authorization to enter has been verified, the proper customs and courtesies will be rendered to the credential holder, and the entry controller will allow the individual to enter the installation.

6.4.4. Unmanned Pedestrian Gates. The minimum standard for controlling physical access to an installation via an unmanned pedestrian gate is:

6.4.4.1. A PACS that can validate a credential to ensure its authenticity plus at least one biometric modality to provide more accurate identification and validate the person is authorized to enter the installation.

6.4.4.2. A pedestrian turnstile that prevents tailgating and ensures only one authorized individual is allowed to enter per credential/biometric validation.

6.4.4.3. Recordable Closed Circuit Television (CCTV) capability that provides 24 hours a day/7 days a week coverage of the unmanned pedestrian gate that's monitored by the BDOC. The CCTV system must be stored in a tamper-resistant or tamper proof system and have the capability to record and store 60 days of video.

6.4.4.4. An intrusion detection system that can provide immediate detection and surveillance capability and alert the BDOC if someone is attempting to bypass the PACS to gain entry to the installation.

6.4.5. Unmanned Installation Entry Control Points. The minimum standard for controlling physical access to an installation via an unmanned entry control point is:

6.4.5.1. An automated PACS that can validate a credential to ensure its authenticity plus at least one biometric modality to provide more accurate identification and validate the person presenting the credential is authorized to enter the installation.

FOR OFFICIAL USE ONLY

6.4.5.2. Anti-tailgating capability that ensures only one authorized vehicle/person is allowed to enter per credential/biometric validation.

6.4.5.3. Recordable Closed Circuit Television (CCTV) capability that provides 24 hours a day/7 days a week coverage of the unmanned entry control point that's monitored by the BDOC. CCTV system must be stored in a tamper-resistant or tamper proof system and have the capability to record and store 60 days of video.

6.4.5.4. An intrusion detection system that can provide immediate detection and surveillance capability and alert the BDOC if someone is attempting to bypass the entry control point to gain entry to the installation.

6.4.5.5. A vehicle barrier system.

6.5. Escort Authority. Escort authority allows an individual, with an authorized form of identification that certifies they have been successfully identity proofed and favorably vetted per this instruction, to vouch for any vehicle occupants, or pedestrians if walking through a pedestrian gate, and escort personnel onto an installation without identity proofing or vetting them. **Note:** Escorted visitors are still subject to any controlled or restricted area limitations, as appropriate. Escorted visitors do not need passes, but must remain with their escort at all times. Sponsored visitors will receive a pass that allows for unescorted entry after vetting and based on sponsorship by authorized/vetted ID card/local pass holders as specified in this AFI.

6.5.1. Military, DoD civilians, military retirees, and adult dependents have escort authority based on the validity of the credential issuance procedures, prior honorable service, or dependency status. **Note:** Installation Commanders will determine escort rules for DoD dependents under the age of 18.

6.5.2. Privatized housing occupants should have the same escort authority as other base residents in their housing area, and will be responsible for their guests. **Note:** The escort authority should be limited to their housing area only.

6.5.3. Contractors, Civilian Retiree Card holders, Non-DoD Federal PIV holders, TWIC holders, PIV-I holders, local pass and card holders (with the exception of privatized housing residents, AFOSI, FBI and USSS agents), approved DoD Privilege card holders, Veterans Identification Card holders, and Foreign National Affiliates with a US DoD CAC are not authorized escort authority.

6.5.4. When rank-neutral PACS, Federal PIV or CAC cards are presented with special agent credentials, after electronic authentication via a PACS that the credential is valid and the person is fit, AFOSI, FBI, and USSS agents have unescorted access to the installation and escort privileges for personnel and official vehicles in all force protection conditions. Paragraphs 6.5.5., 6.5.11., and 6.5.13. do not apply to AFOSI, FBI and USSS agents.

6.5.5. Installation Commanders will determine the number of personnel that approved escorts are authorized to escort.

6.5.5.1. **(Added-ANG)** The number of personnel authorized to be escorted will not exceed that of which a normal person could reasonably maintain surveillance and control. The NGB recommendation is not to exceed five persons per escort.

6.5.5.2. **(Added-ANG)** Escorts will only be permitted to escort a single vehicle in addition to their own. Exceptions may be granted by the Installation Commander to support mission requirements.

6.5.6. The Installation Commander may delegate escort approval authority to the unit commander level at his or her discretion and will document these authorities and processes in the IDP. Escort privileges will be annotated on the locally issued access credential.

6.5.7. Members escorting personnel are entirely responsible for the actions of all occupants in their vehicle or pedestrians if walking, and for meeting all security requirements for escort as established by the Installation Commander.

6.5.8. Personnel escorted within the installation must stay within the physical custody of the sponsor, within the sponsor's residence, or the adjacent, immediate public areas of the sponsor's residence. Escorted individuals must remain in the control of the escort.

6.5.8. **(ANG)** Escorts are required to immediately report loss of contact with person(s) being escorted to BDOC. Reports will include the name and description of the escorted individual/vehicle, the purpose of the visit, and last known location/direction of travel.

6.5.9. Escort authority does not authorize vehicle occupants, or pedestrians if walking, to enter internal controlled, restricted, limited, or exclusion areas without first meeting all security requirements and procedures for those areas.

6.5.10. Escort authority members may only vouch for individuals riding in the immediate vehicle they are operating, or immediate area if they are walking.

6.5.11. Escort authority members are not authorized to vouch for non-US individuals (non U.S. citizens/non U.S. permanent resident aliens) to include those with foreign passports or identification credentials. All foreign visitors must have a visitor pass and present it to the entry controller.

6.5.12. Commanders may suspend escort authority based on the local threat or may revoke individual escort authority privileges at their discretion.

6.5.13. Escort authority privileges are automatically suspended at FPCON Charlie. Installations will ensure installation access control plans/procedures reflect when escort authority is suspended.

6.5.14. Installations should identify a means of determining duress of escort authority members when implementing the policy. Installations should conduct locally determined duress checks.

6.5.14. **(ANG)** Restricted Area duress codes/words will not be publicized or utilized by the general base population as a procedure to identify duress of an installation escort authority. Consider using a procedure such as verbal verification of information contained on the escort's identification as an authenticator (e.g. please verify your date of birth).

6.6. Sponsorship. Sponsorship allows approved individuals affiliated with the DoD to take responsibility for verifying and authorizing an applicant's need for a locally produced identification credential to facilitate unescorted access to an installation.

6.6.1. Active Duty, Guard and Reserve personnel on official orders, CAC holders (to include Contractor CAC holders), and dependents are authorized to sponsor individuals onto an

FOR OFFICIAL USE ONLY

installation they are affiliated with/assigned to. Foreign National Affiliates with a US DoD CAC are authorized to sponsor individuals onto the installation in accordance with Foreign Visit System regulations and MAJCOM guidance. Per the guidance in this instruction, individuals sponsored by Foreign National Affiliates must be identity proofed and vetted prior to the issuance of a temporary visitor pass. **Note:** Installation Commanders will determine sponsorship rules for DoD dependents under the age of 18.

6.6.2. Privatized housing residents with locally issued credentials are authorized to sponsor individuals onto an installation they are affiliated with/assigned to, but sponsorship privileges should be limited to their particular housing area only.

6.6.3. Installation bank and credit union employees with locally issued credentials are authorized to sponsor individuals onto the installation they are affiliated with/assigned to.

6.6.4. Active Duty, Guard and Reserve personnel on official orders, and CAC holders who are on official TDY orders to an installation are authorized to sponsor individuals onto that installation only for the duration of their TDY/Active Duty orders.

6.6.5. Installation Commanders shall establish further guidelines/restrictions concerning the numbers of visitors that may be sponsored, times of day, length of time the locally issued credential can be issued for, and other restrictions as appropriate and codify into local guidance. Additionally, Installation Commanders have the flexibility to include sponsorship privileges for unique categories not addressed in this AFI.

6.7. Installation Perimeter Access Control Procedures for Emergency Responders and Civilian Law Enforcement. Installations will develop procedures for first responders' installation access control during emergencies and authorized purposes (e.g. civilian law enforcement serving a warrant). This includes, but is not limited to, law enforcement, medical and fire department personnel. All procedures need to be approved by the Installation Commander and codified in local instructions/plans.

6.8. Internal Access (to include Service-determined controlled, restricted, and limited areas). Validating a need for installation access will not automatically establish access requirements for internal areas.

6.8.1. MAJCOMS and installations, through implementing instructions, will ensure area, facility, and room owners (separate from external access) conduct their own assessment and validate an individual's need for internal access based on locally determined threats and vulnerabilities, criticality of assets/information present, assumption of risk, and directives relating to internal security measures.

6.8.1. (ANG) Base escort authority does not authorize vehicle occupants, or pedestrians if walking, to enter internal controlled, restricted, limited, or exclusion areas without first meeting all security requirements and procedures for those areas. Established entry control procedures for these areas will be strictly adhered to.

6.8.2. Internal access requirements are specified within AFI 31-101.

6.9. Identification/Verification. Law and Order or issuance personnel may require an individual to provide his or her biometric information for identification-verification purposes.

6.9.1. When the request for biometric information extends beyond identifying an individual, “probable cause” or other legal basis must be present before any apprehension is made or search conducted.

6.9.1. (ANG) This requirement does not prevent a Security Forces member from performing a protective frisk when the member reasonably believes a person is armed and presently dangerous to the member or others IAW AFMAN 31-201V2, *Legal Considerations*, paragraph 1.3.3.

6.9.2. If the request for the biometric information leads to an apprehension or search, coordination with a representative of the servicing judge advocate office should occur.

6.9.3. If the apprehension or search involves a foreign host-nation citizen, coordination with the host-nation police will occur.

6.9.4. Refusal to provide biometric information may be the basis for immediate surrender of the individual’s locally produced access credential or DoD ID card and grounds for further administrative or punitive action by the command.

Chapter 7

IDENTITY MANAGEMENT ENTERPRISE SERVICES ARCHITECTURE

7.1. Source Documents.

7.1.1. Section 1069 of the 2008 National Defense Authorization Act (NDAA), now Public Law 110-181, mandates the Secretary of Defense develop protocols to determine fitness of individuals entering an installation and standards and methods for verifying the identity of individuals. To ensure a person who was initially issued a credential is still fit to enter an installation, continuous information management from authoritative data sources is required.

7.1.2. DTM 09-012 mandates PACS support a “DoD-wide and federally interoperable” access control capability that can authenticate United States Government (USG) physical access credentials and support access enrollment, authorization processes, and secure information sharing.

7.2. Identity Management Enterprise Services Architecture Requirements.

7.2.1. To meet DTM 09-012, the DoD is developing an Identity Management Enterprise Services Architecture that enables PACS to rapidly, electronically and securely authenticate approved physical access credentials, provide continuous information management against authoritative data sources, and support access enrollment, authorization processes and secure information sharing throughout the DoD and authorized Federal Agencies to enable Installations/Organizations to authenticate credentials and an individual’s authorization and fitness to enter.

7.2.2. Authoritative Databases.

7.2.2.1. The DoD is looking to incorporate portions of the following databases into the Identity Management Enterprise Services Architecture to ensure installation leadership has the data they needed to determine if a person is authorized and fit to enter an installation. **Note:** More authoritative/governmental databases will be incorporated in the future as mission needs dictate.

7.2.2.1.1. DEERS. Contains records pertaining to active duty and reserve military and their family members, military retired, DoD civilian service personnel, DoD contractors and Foreign and Civilian applicants authorized a RAPIDS produced credential. DEERS is comprised of the National Enrollment Database (NED), the Person Data Repository (PDR), and several satellite databases. This system provides accurate and timely information support for DoD ID smart cards, provides benefit eligibility information for all Service members and their families, supports Teslin ID cards, unique identities and will be the foundation of the Enterprise attributes services for real time Attribute Based Access Control for the DoD.

7.2.2.1.2. NCIC.

7.2.2.1.2.1. Computerized index of criminal justice information (i.e. criminal record history information, fugitives, stolen properties, missing persons). It is available to Federal, state and local law enforcement and other criminal justice agencies.

7.2.2.1.2.2. The Identity Management Enterprise Services Architecture will utilize the authoritative federal wants & warrants list and compare this data against information stored in access control authorization lists.

7.2.2.1.3. TSDB.

7.2.2.1.3.1. Contains the US Government's comprehensive database of both international and domestic terrorist identity information.

7.2.2.1.3.2. The Identity Management Enterprise Services Architecture will utilize the authoritative terrorist watch list and compare this data against information stored in access control authorization lists.

7.2.2.1.4. Consolidated DoD Law Enforcement Database. Consolidated DoD law enforcement data available to support authorized requirements by providing information critical to determine fitness to enter an installation.

7.2.2.1.5. TWIC Database. TWIC database will provide information on certificate revocation lists to ensure a TWIC credential is still valid.

7.2.2.1.6. Non-DoD Federal PIV Database. Non-DoD Federal PIV Database will provide information of Public Key Infrastructure (PKI) certification revocation lists to ensure a Non-DoD Federal PIV is still valid.

7.2.2.1.7. DoD ABIS. Provides the store, match, share capability for the biometrics enterprise on all non-US enrollments. Tactical collection devices such as Biometrics Automated Toolset (BAT), Biometric Identification System for Access (BISA), DBIDS, and Secure Electronic Enrollment Kit (SEEK) provide enrollment data to the ABIS which matches those enrollments against existing enrollments and recovered latent fingerprint files and provides a match result back to the enroller and the Intel Community.

7.2.2.1.8. IDProTECT. Transitions proven capabilities into an operational biometric enterprise.

7.2.2.1.9. New Database Requirements. As new governmental/authoritative data sources come on line, the Identity Management Enterprise Services Architecture will incorporate them, as applicable.

7.3. Continuous Information Management Capability.

7.3.1. Continuous information management of authoritative, governmental data sources is required to ensure a person is still authorized and fit to enter an installation after the initial identity proofing and vetting is accomplished to meet the mandates in Section 1069 of the 2008 NDAA, now public law 110-181.

7.3.2. The Identity Management Enterprise Services Architecture is being designed to provide this capability.

Chapter 8

BIOMETRICS

8.1. Overview. Biometrics is an important enabler that should be fully integrated into the conduct of Air Force activities to support the full range of military operations.

8.1.1. The physical and cyberspace threats facing AF personnel, infrastructures and networks continue to evolve and have increasing ability to disrupt military operations.

8.1.2. In order to operate effectively, the AF will continue to rely on information assurance and identity management capabilities.

8.1.3. Biometric technologies provide the next evolutionary step in AF Identity Management as they have the capability to provide faster, more accurate identification and authentication validation.

8.1.4. The use of one or more biometric modalities via a biometric system improves the opportunity to verify identification with increasingly higher probabilities of success.

8.1.5. Biometric System. A system capable of capturing a biometric sample from a subject; extracting and processing the biometric data from that sample; storing the extracted information in a database; comparing the biometric with data contained in one or more references; matching, and indicating whether or not an identification or verification of identity has been achieved.

8.1.6. Biometric activities within the DoD are organized under the BIMA, formerly the Biometrics Task Force (BTF), in accordance with DoD Directive 8521.01E, *Department of Defense Biometrics*.

8.1.6.1. The BIMA leads DoD activities to program, integrate, and synchronize Biometric technologies and capabilities and to operate and maintain DoD's authoritative Biometric database to support the National Security Strategy.

8.1.6.2. The BIMA serves to deliver capabilities to increase Joint Service interoperability and to empower the warfighter by improving operational effectiveness on the battlefield.

8.1.6.3. The Secretary of the Army is the designated Executive Agent (EA) for DoD Biometrics. The BIMA executes EA responsibilities as the Executive Manager.

8.1.6.4. The Secretary of the Air Force Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6) provides overarching guidance on Biometrics, including investment and integration planning in accordance with the existing DoD biometrics governance structure.

8.1.6.5. This collaboration will provide greater accountability and ensure biometric applications are technically capable and operationally synchronized to comply with DoD-approved architecture, standards, and processes.

8.2. Requirements. Commanders at all levels are authorized to use biometric systems to collect biometric data (e.g., face, finger, palm, iris, DNA, voice, other modalities) required to enroll and verify the identification of all personnel who request or require access to DoD systems, services, and facilities. This includes:

FOR OFFICIAL USE ONLY

8.2.1. Identity Proofing.

8.2.1.1. Collecting, registering and matching biometrics stored in a blue force (friendly) database to verify the identification of personnel and authorization to access DoD installations/facilities as part of the identity proofing process.

8.2.1.2. In addition to utilizing biometrics for access control on a daily basis, if mission needs dictate, biometrics may also be useful for:

8.2.1.2.1. Increased FPCONS. During increased FPCONS, when the population authorized access to the installation is reduced, biometrics that provide greater identity management accuracy will greatly enhance force protection by limiting access to only authorized personnel.

8.2.1.2.2. RAMs. Unpredictability in security activities is one of the best and most effective deterrents available to a commander. Randomly changing security/force protection measures by utilizing biometric access controls as a RAM enables integrated defenses to appear formidable and prevents threats from easily discerning and predicting patterns or routines that are vulnerable to attack.

8.2.1.2.3. Lost Credentials. Enabling authorized credential holders to gain access to the installation/facility via their biometric to ensure no mission degradation.

8.2.2. Matching.

8.2.2.1. Air Force personnel engaged in identity management are authorized the use of biometric processes to increase the accuracy and speed of identification management by acquiring, storing and analyzing biometric modalities to determine fitness to enter an installation as part of the vetting process.

8.2.2.2. DoD ABIS-Red Force Database. Provides the store, match, share capability for the biometrics enterprise on all non-US enrollments. Tactical collection devices such as BAT, BISA, DBIDS, and SEEK provide enrollment data to the ABIS which matches those enrollments against existing enrollments and recovered latent fingerprint files and provides a match result back to the enroller and the Intel Community.

8.3. Biometric Categories. In regards to biometrics, for the purposes of this instruction, personnel are categorized in two groups: DoD and Non-DoD Persons.

8.3.1. DoD Persons. Consists of military (Active, Guard and Reserves), government civilians, military dependents, military retirees, and other groups of official government Identification Card holders.

8.3.1.1. Biometrics collected for this group may be stored in the approved DoD database, matched against authoritative databases and shared among DoD agencies.

8.3.1.2. All Biometric data and associated information collected as a result of DoD operations or activities shall be maintained and controlled by DoD, unless otherwise specified by the DoD EA for Biometrics.

8.3.1.3. Storage and retention of biometric data in this category must be consistent with the applicable (System of Records Notices) and applicable records disposition schedules.

8.3.2. Non DoD Persons. Consists of contractors, visitors, and temporary workers.

8.3.2.1. Biometrics collected for this group may be matched against authoritative databases, and stored temporarily in a USAF approved local database.

8.3.2.2. Storage and retention of biometric data in this category must be consistent with the applicable (System of Records Notices) and applicable records disposition schedules.

8.4. Biometric Standards.

8.4.1. Any biometrics procedures will comply with applicable Federal privacy laws as found in DoD and AF regulations and instructions regarding privacy and biometrics.

8.4.2. Biometric collection, transmission, storage, caching, tagging and use shall be controlled through the use of DoD-approved national, international, and other consensus-based standards, protocols, best practices, and equipment to ensure consistency and support interoperability.

8.4.3. All biometric data and associated information collected as a result of DoD operations or activities shall be maintained or controlled by the DoD, unless otherwise specified by the DoD EA for DoD Biometrics.

8.4.4. The DoD ABIS was designed to be similar to the FBI Criminal Justice Information Services (CJIS) IAFIS, and therefore its interface was based on the FBI's Electronic Fingerprint Transmission Specification (EFTS). Because of the different nature of DoD encounters and detainment circumstances, the DoD has additional operational requirements beyond those defined in the FBI EFTS.

8.4.4.1. The DoD-unique capabilities are defined in *DoD Electronic Biometric Transmission Specification (EBTS) Version 2.0*.

8.4.4.2. The *DoD EBTS Version 2.0* is a transmission specification to be used between DoD systems that capture biometric data and repositories of biometric data.

8.4.4.3. This document should be used by program managers, trainers, or other system design personnel to gain an understanding of the capabilities enabled by the DoD EBTS.

8.5. Local Guidance Requirements.

8.5.1. Before biometrics are utilized on an installation, the procedures must be codified in a local instruction, coordinated with the servicing legal office and approved by the installation commander (or equivalent authority). Additionally, installations must ensure all applicable SORNs are published.

8.5.2. Biometric collection on foreign visitors is authorized only if coordinated with the servicing legal office and approved by the installation commander (or equivalent authority). Installation Commanders will determine if this is a requirement based on unique mission requirements, base vulnerabilities and threat conditions.

8.5.3. The minimum age requirement to collect a biometric is 10 years old, to match the standard age at which a dependent can receive an ID card per AFI 36-3026 (IP), Volume 1. **Note:** children under age 10 can receive an ID card if the issuing Site Security Manager or Super Verifying Official determine unique or extenuating circumstances warrants it.

Chapter 9

TRAINING AND EXERCISES

9.1. Concept. Individual and team training, individual certification, and the use of realistic exercises ensure entry control personnel understand their responsibilities and are ready to perform their duties. The minimum standards outlined below do not negate standardized training and certification requirements associated with the security forces career field.

9.2. Training. Training and certification, when applicable and required, are pivotal to effective access control operations.

9.2.1. Installation Entry Controllers will:

9.2.1.1. Be trained on local threats/enemy tactics, techniques, and procedures (TTPs), visual identification/authentication of access credentials, detection of stolen/improperly registered vehicles, professional interaction with visitors, and USAF and local access control guidance (debarments, entry authority lists, etc.).

9.2.1.2. Be certified on the use of all local physical access control equipment to include, but not limited to, the use of and employment of barrier systems and PACS.

9.2.2. Visitor Center Personnel will:

9.2.2.1. Be trained on the inspection and use of ID proofing documents and the registration and issuance of access credentials.

9.2.2.2. Meet all federal, state, or system-specific training and certification requirements for accessing authoritative government databases.

9.2.2.3. Be trained and certified on the protection of PII as it relates to the collection, storage, transmission, sharing, and use of biographic and biometric information.

9.2.3. Vehicle Searches. All personnel conducting searches on vehicles will be trained and certified pursuant to the technologies employed and in accordance with Security Forces TTPs.

9.3. Exercises. Defense Force Commanders will ensure entry control personnel conduct exercises with a group of penetration testers and plausible scenarios designed to instill effectiveness in neutralizing potential threats and emergency situations and assess the effectiveness of measures.

9.3.1. Scenarios could include, but are not limited to, attempted breaches of access control facilities and installations, fraudulent identification, weapons employment, vehicle/pedestrian borne improvised explosive devices, surveillance of friendly TTPs, and first responder entry/exit.

9.3.2. MAJCOM A7S will determine the rate and frequency of exercises.

9.3.2.1. **(Added-ANG)** Each ANG installation will conduct a minimum of two Installation Level access control exercises annually on each duty flight. Exercises will be documented in the AF Form 53, Security Forces Desk Blotter.

FOR OFFICIAL USE ONLY

9.3.2.2. **(Added-ANG)** Unit Standardization and Evaluation sections will be responsible for conducting access control exercises as a flight level exercise. Results will be documented. Provide reports and trend analysis to the DFC.

9.4. Lessons Learned, Vulnerabilities, and Higher Headquarters Feedback. Not only do training and exercises ensure capable entry control teams, but they facilitate the identification of USAF and local vulnerabilities in access control processes and policies.

9.4.1. Units will analyze and report significant access control incidents that occur during SF operations to include, but not limited to exercises, special events, deployments and daily operations.

9.4.2. Units will provide After Action Reports in accordance with AFI 31-201, *Security Forces Standards and Procedures*, 30 Mar 2009.

9.4.2. **(ANG)** ANG units will provide After Action Reports (AAR) via the ANG Security Forces Joint Lessons Learned Information System (JLLIS) website.

LOREN M. RENO, Lt General, USAF
DCS/Logistics, Installations, and Mission Support

(ANG)

Harry M Wyatt III, Lieutenant General, USAF
Director, Air National Guard

FOR OFFICIAL USE ONLY

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFDD 2-4, *Combat Support*, 23 March 2005

AFDD 2-4.1, *Force Protection*, 9 November 2004

AFH 10-2401, *Vehicle Bomb Mitigation Guide*, 1 September 2006

AFI 10-245, *Antiterrorism (AT)*, 30 March 2009

AFI 10-1004, *Conducting Air Force Open Houses*, 18 February 2010

AFI 14-119, *Intelligence Support to Force Protection (FP)*, 15 August 2007

AFI 16-107, *Military Personnel Exchange Program (MPEP)*, Certified Current, 23 April 2010

AFI 16-201, *Air Force Foreign Disclosure and Technology Transfer Program*, Incorporating Change 1, 11 August 2009

AFI 31-101, *Integrated Defense*, Incorporating Change 1, 20 September 2010

AFI 31-201, *Security Forces Standards and Procedures*, 30 March 2009

AFI 31-203, *Security Forces Management Information Systems*, 29 July 2009

AFI 31-207, *Arming and Use of Force by Air Force Personnel*, 29 January 2009

AFI 31-211(I), *Army and Air Force Exchange Service Operations*, 30 July 2008

AFI 31-501, *Personnel Security Program Management*, 27 January 2005

AFI 32-6007, *Privatized Family Housing*, 22 June 2005

AFI 33-200, *Information Assurance (IA) Management*, Incorporating Through Change 2, 15 October 2010

AFI 33-321, *Authentication of Air Force Records*, 3 August 2011

AFI 33-332, *Air Force Privacy Program*, 16 May 2011

AFI 34-211(I), *Army and Air Force Exchange Service Operations*, 30 July 2008

AFI 36-102, *Basic Authority and Responsibility for Civilian Personnel Management and Administration*, 18 February 1994

AFI 36-507, *Mobilization of the Civilian Work Force*, 21 July 1994

AFI 36-2225, *Security Forces Training and Standardization Evaluation Programs*, 28 April 2009

AFI 36-3026 (IP), Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, 17 June 2009

AFI 71-101, Volume 1, *Criminal Investigations*, Incorporating Change 1, 17 March 2009

AFJI 31-102, *Physical Security*, 31 May 1991

AFMAN 31-201 Volume 7, *Security Forces Administration and Reports*, 28 August 2009

FOR OFFICIAL USE ONLY

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPD 16-1, *International Affairs*, 2 November 2009

AFPD 31-1, *Integrated Defense*, 7 Jul 2007; Incorporating Change 1, 22 April 2009

AFTTP 3-10.1, *Integrated Base Defense (IBD)*, 20 August 2004

AFTTP 3-10.2, *Integrated Base Defense Command and Control*, 1 March 2008

AFTTP 3-31.1, *Entry Control*, 29 May 2007

Biometrics Task Force, *DoD Electronic Biometric Transmission Specification*, Version 2.0, 27 March 2009

Defense Information Systems Agency, *Secure Remote Computing Security Technical Implementation Guide Version 1, Release 2*, 10 August 2005

Deputy Secretary of Defense Memorandum, *Policy Guidance for Provision of Medical Care for Department of Defense Civilian Employees Injured or Wounded While Forward Deployed in Support of Hostilities*, 24 September 2007

Directive Type Memorandum (DTM) 07-015-USD(P&R), *DoD Social Security Number (SSN) Reduction Plan*, 28 March 2008

Directive Type Memorandum (DTM) 08-003-USD(P&R), *Next Generation Common Access Card (CAC) Implementation Guidance*, Incorporating Change 1, 10 August 2010

Directive Type Memorandum 08-006, *DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12)*, 26 November 2008

Directive Type Memorandum 09-012, *Interim Policy Guidance for DoD Physical Access Control*, 8 December 2009

DoD, *Electronic Biometric Transmission Specification (EBTS) Version 2.0*, 27 March 2009

DoD 1400.25-M, *DoD Civilian Personnel Manual*, 1 December 1996

DoD 1400.25-M, *Civilian Personnel Manual*, Subchapter 1231, *Employment of Foreign Nationals*, December 1996

DoD 5200.08-R, *Physical Security Program*, 9 Apr 2007, Incorporating Change 1, 27 May 2009

DoD 5400.11-R, *Department of Defense Privacy Program*, 14 May 2007

DoDD 1404.10, *DoD Civilian Expeditionary Workforce*, 23 January 2009

DoDD 5015.2, *DoD Records Management Program*, 6 March 2000

DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*, 7 January 1980

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, 22 June 2005

DoDD 5400.11, *Department of Defense Privacy Program*, 8 May 2007

DoDD 8521.01E, *Department of Defense Biometrics*, 21 February 2008

DoDI 1000.13, *Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals*, 5 December 1997

FOR OFFICIAL USE ONLY

DoDI 1330.21, *Armed Services Exchange Regulations*, 14 July 2005

DoDI 3224.03, *Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)*, 1 October 2007

DoDI 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information*, 9 October 2008

DoDI 5200.8, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB), Incorporating Change 1*, 19 May 2010

DoDI 5400.16, *DoD Privacy Impact Assessment (PIA) Guidance*, 12 February 2009

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007

Executive Order 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Controlled National Security Information*, 30 June 2008

Federal Information Processing Standards Publication 201-1, *Personal Identity Verification for Federal Employees and Contractors*, March 2006

Handbook for Employers, Instruction for Completing Form I-9 (Employment Eligibility Verification Form), U.S. Department of Homeland Security, U.S. Citizenship and Immigration Services. M-274 (Rev. 04/03/09) N

Homeland Security Presidential Directive-6, *Integration and Use of Screening Information*, 16 September 2003

Homeland Security Presidential Directive-11, *Comprehensive Terrorist-Related Screening Procedures*, 27 August 2004

Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, 27 August 2004

Homeland Security Presidential Directive-24, *Biometrics for Identification and Screening to Enhance National Security*, 5 June 2008

HR 4954, *Security and Accountability for Every (SAFE) Port Act of 2006*, 3 January 2006

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 Apr 2001 (as amended through 17 March 2009)

Joint Publication 3-07.2, *Antiterrorism*, 14 April 2006

Joint Publication 3-10, *Joint Security Operations in Theater*, 1 August 2006

Joint Publication 4-10, *Operational Contract Support*, 17 October 2008

National Institute of Standards and Technology (NIST) Publication 800-63, *Electronic Authentication Guideline*, April 2006

National Institute of Standards and Technology (NIST) Publication 800-73, *Interfaces for Personal Identity Verification (PIV) (Parts 1-4)*, September 2008

National Institute of Standards and Technology (NIST) Publication 800-76, *Biometric Data Specifications for Personal Identity Verification (PIV)*, January 2007

National Institute of Standards and Technology (NIST) Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008

National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management, *NSTC Policy for Enabling the Development, Adoption, and Use of Biometrics Standards*, 7 September 2007

Office of Management and Budget Memorandum (M-04-04), *E-Authentication Guidance for Federal Agencies*, 16 December 2003

Office of Management and Budget Memorandum (M-05-24), *Implementation of Homeland Security Presidential Directive-12-Policy for a Common Identification Standard for Federal Employees and Contractors*, 5 August 2005

Physical Access Interagency Interoperability Working Group, *Technical Implementation Guidance: Smart Card Physical Access Control Systems, Version 2.2*, 30 July 2004

Presidential Memorandum, *Controlled Unclassified Information*, 4 November 2010

Privacy Act of 1974

Public Law 77-140 (1941)

Public Law 79-51 (1945)

Public Law 107-71, *Aviation and Transportation Security Act*, 19 November 2001

Public Law 107-295, *Maritime Transportation Security Act of 2002*, 25 November 2002

Section 1069 of Public Law 110-181, *National Defense Authorization Act or Fiscal Year 2008*, 28 January 2008

System of Records Notices (SORN) F031 AF SF B, *Security Forces Management Information System (SFMIS)*, F031 AF SP F, *Notification Letters to Persons Barred from Entry to Air Force Installations*, June 11, 1997; and F031 AF SP O, *Documentation for Identification and Entry Authority*, 11 June 1997

Title 5, United States Code, Section 2105

Title 10, United States Code, Chapter 1223

Title 10, United States Code, Section 1408(h)

Title 10, United States Code, Section 10147

Title 18, United States Code, Section 1382

Title 31, United States Codes, Sections 6303, 6304 and 6305

Title 33, United States Code, Section 857-4

Title 44, United States Code, Section 3542(b)(2)

Title 50, United States Code, Section 797, *Internal Security Act of 1950*

Unified Facilities Criteria 3-260-01, *Airport and Heliport Planning and Design*, 17 November 2008

Unified Facilities Criteria 3-535-01, *Visual Air Navigation Facilities*, 17 November 2005

Unified Facilities Criteria 4-022-01, *Security Engineering: Entry Control Facilities/Access Control Points*, 25 May 2005

Unified Facilities Guide Specifications, Electronic Security System, Electronic Security Center, Section 13720A, October 2007

USAF Chief of Staff (CSAF) memorandum dated 3 March 2004 (SUBJ: *Protect the Force: Establishing the New Baseline Force Protection Posture*)

USAF Vice Chief of Staff (VCSAF) memorandum dated 8 September 2009 (SUBJECT: *Air Force Policy for Installation Access Control*)

Prescribed Forms

None

Adopted Forms

AF Form 75, *Visitor/Vehicle Pass*, 1 June 2002

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

DD Form 2, *United States Uniformed Services Identification Card (Retired)*,

DD Form 2, *Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Red)*

DD Form 2, *Armed Forces of the United States Geneva Conventions Identification Card (Reserve) (Green)*

DD Form 2, *United States Uniformed Services Identification Card (Reserve Retired)*

DD Form 1173, *Uniformed Services Identification and Privilege Card*

DD Form 1173-1, *Department of Defense Guard and Reserve Dependent Identification Card*

DD Form 1934, *Geneva Conventions Identity Card for Medical and Religious Personnel Who Serve in or Accompany the Armed Forces*

DD Form 2764, *United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card (Machine-readable card)*

DD Form 2765, *Department of Defense/Uniformed Services Identification and Privilege Card*

DD Form 2930, *Privacy Impact Assessment*

Abbreviations and Acronyms

ABIS—Automated Biometric Identification System

AF—Air Force

AFB—Air Force Base

AFCEA—Air Force Civil Engineer Support Agency

FOR OFFICIAL USE ONLY

AFDD—Air Force Doctrine Document
AFH—Air Force Handbook
AFI—Air Force Instruction
AFMAN—Air Force Manual
AFOSI—Air Force Office of Special Investigations
AFPD—Air Force Policy Directive
AFRC—Air Force Reserve Command
AFRIMS—Air Force Records Information Management System
AFSFC—Air Force Security Forces Center
AFTTP—Air Force Tactics, Techniques and Procedures
AO—Area of Operations
AT—Antiterrorism
BAT—Biometrics Automated Toolset
BDOC—Base Defense Operations Center
BIDS—Biometric Identification System (USFK)
BIMA—Biometrics Identity Management Agency
BISA—Biometric Identification System for Access
BTF—Biometric Task Force
C2—Command and Control
CAC—Common Access Card
CAK—Card Authentication Key
CBRNE—Chemical, Biological, Radiological, Nuclear and High-Yield Explosive
CCDR—Combatant Commander
CCTV—Closed Circuit Television
CHUID—Cardholder Unique Identifier
CI—Counterintelligence
CJIS—Criminal Justice Information Services
CM—Confirmation Module
COCO—Contractor-Owned, Contractor-Operated
COCOM—Combatant Command
CONUS—Continental United States (Within)
CSAF—Chief of Staff of the United States Air Force

FOR OFFICIAL USE ONLY

CUI—Controlled Unclassified Information
DAF—Department of the Air Force
DBIDS—Defense Biometric Identification System
DEERS—Defense Enrollment Eligibility Reporting System
DFC—Defense Force Commander
DHRA—Defense Human Resources Activity
DHS—Department of Homeland Security
DOD—Department of Defense
DODD—Department of Defense Directive
DODI—Department of Defense Instruction
DOS—Department of State
DRU—Direct Reporting Unit
DTM—Directive Type Memorandum
EA—Executive Agent
EAL—Entry Authority List
EBTS—Electronic Biometric Transmission Specification
ECP—Entry Control Point
EE—Emergency Essential
EFTS—Electronic Fingerprint Transmission Specification
EM—Emergency Management
EOD—Explosive Ordnance Disposal
FBI—Federal Bureau of Investigation
FIPS—Federal Information Processing Standards
FOA—Field Operating Agency
FOUO—For Official Use Only
FP—Force Protection
FPCON—Force Protection Condition
FSS—Force Support Squadron
FVS—Foreign Visits System
FVS—CM—Foreign Visits System Confirmation Module
GIG—Global Information Grid
GO—General Orders

FOR OFFICIAL USE ONLY

GOCO—Government-Owned, Contractor-Operated

HAF—Headquarters Air Force

HN—Host Nation

HQ—Headquarters

HQ AFCEA—Headquarters, Air Force Civil Engineer Support Agency

HQ AFRC—Headquarters, Air Force Reserve Command

HQ AFSFC—Headquarters, Air Force Security Forces Center

HQ NGB—CF—Headquarters, Air National Guard Bureau

HSPD—Homeland Security Presidential Directive

IAFIS—Integrated Automated Fingerprint Identification System

IAW—In Accordance With

ICC—Integrated Circuit Chip

ID—Identification

IDC—Integrated Defense Council

IDM—Identity Management

IDP—Integrated Defense Plan (see also ISP)

IDRMP—Integrated Defense Risk Management Process

III—Interstate Identification Index

INS—Immigration and Naturalization Service

IPO—Information Protection Office

IR—Infrared

IT—Information Technology

MAJCOM—Major Command

METL—Mission Essential Task List

METTTTC—Mission, Enemy, Terrain and Weather, Troops and Support Available-Time Available and Civil Considerations

MPEP—Military Personnel Exchange Program

MSC—Military Sealift Command

MSO—Military Service Obligation

MTSA—Maritime Transportation Security Act

MWD—Military Working Dog

MWR—Morale, Welfare, and Recreation

NACI—National Agency Check With Written Inquiries

FOR OFFICIAL USE ONLY

NAF—Non-appropriated fund
NARA—National Archives and Records Administration
NATO—North Atlantic Treaty Organization
NCIC—National Crime Information Center
NDAA—National Defense Authorization Act
NED—National Enrollment Database
NIPRNET—Non-Classified Internet Protocol Router Network
NOAA—National Oceanic Atmospheric Administration
OCONUS—Outside the Continental United States
OET—Other Eligible Tenants
OMB—Office of Management and Budget
OPCON—Operational Control
OPLAN—Operation Plan
OPM—Office of Personnel Management
OPR—Office of Primary Responsibility
PACS—Physical Access Control System
PDR—Person Data Repository
PDRL—Permanent Disability Retired List
PIA—Privacy Impact Assessment
PII—Personally Identifiable Information
PIN—Personal Identification Number
PIV—Personal Identity Verification
PIVI—Personal Identity Verification-Interoperable
PKI—Public Key Infrastructure
POM—Program Objective Memorandum
POV—Privately Owned Vehicle
POW—Prisoner of War
PSEAG—Physical Security Equipment Action Group
RAM—Random Antiterrorism Measure
RAPIDS—Real-Time Automated Personnel Identification System
RDS—Records Disposition Schedule
RDT&E—Research, Development, Test and Evaluation

FOR OFFICIAL USE ONLY

RIEVC—Random Installation Entry/Exit Vehicle Checks
ROE—Rules of Engagement
ROTC—Reserve Officer Training Corps
RTAP—Reserve Transition Program
SAF—Secretary of the Air Force
SAF/IAPD—Secretary of the Air Force, Foreign Disclosure and Technology Transfer Division
SAF/XCI—Secretary of the Air Force, Information Services and Integration
SEEK—Secure Electronic Enrollment Kit
SF—Security Forces
SFMIS—Security Forces Management Information System
SFOP—Police Services Branch
SFXR—Requirements Branch
SJA—Staff Judge Advocate
SOFA—Status of Forces Agreement
SORN—System of Records Notices
SSA—Social Security Administration
SSB—Special Separation Benefit
SSN—Social Security Number
TA—Transition Assistance
TAD—Temporary Assigned Duty
TAMP—Transition Assistance Management Program
TDRL—Temporary Disability Retired List
TDY—Temporary Duty
TSA—Transportation Security Administration
TSDB—Terrorist Screening Database
TTP—Tactics, Techniques and Procedures
TWIC—Transportation Worker Identification Credential
UCMJ—Uniform Code of Military Justice
UFC—Unified Facilities Criteria
US—United States
USAF—United States Air Force
USC—United States Code

FOR OFFICIAL USE ONLY

USD(I)—Under Secretary of Defense for Intelligence

USDP&R—Under Secretary of Defense for Personnel and Readiness

USFJ—United States Forces Japan

USFK—United States Forces Korea

USG—United States Government

USO—United Service Organizations

USPHS—U.S. Public Health Service

USS—United Seaman's Service

UV—Ultraviolet

VCSAF—Vice Chief of Staff of the Air Force

VO—Verifying Official

VPN—Virtual Private Network

VSI—Voluntary Separation Incentive

Terms

Access Control—The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances). A function or a system that restricts access to authorized persons only.

Access Control List—A list containing (at a minimum) the names of individuals authorized access and their subsequent authorities of sponsorship (e.g., privileges, times and/or dates for access, unescorted or escorted designation). In an electronic PACS, these items are logically stored in the PACS database.

Access Credential—A physical artifact issued by the Federal, State or local government that attests to one's right to credit or authority. The access credential contains and/or depicts characteristics, authorizations, and privileges for physical access and internal security controls.

Access to a DoD Network—User logon to a Windows active directory account on the NIPRNet or an authorized network operating system account on the NIPRNet.

Access to a DoD Network (remote)—Authorized NIPRNet users accessing a NIPRNet resource from:

Another NIPRNet resource outside of the originating domain.

An authorized system that resides outside of the NIPRNet. This includes domain-level access from handheld devices. Remote access includes logon for the purposes of tele-work, Virtual Private Network (VPN), and remote administration by DoD or non-DoD personnel.

Adopted Child—A child adopted before the age of 21 or if enrolled in a full-time course of study at an institution of higher learning before the age of 23. Except for entitlement to medical care, a child with an incapacitating condition that existed before the age of 21 or that occurred while the child was a full-time student prior to the age of 23 may be adopted at any age provided

it is determined that there is a BONA FIDE parent child relationship. A child of an active duty member or retiree who is adopted by a nonmilitary member after the death of the sponsor remains eligible for medical care only as there would be no termination of the legal relationship between the child and the deceased sponsor.

Annunciation—The term “annunciation” (or annunciate) is the act of a sound or display indicator announcing which sensor has detected a change in state.

Antiterrorism (AT)—Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces. (JP 1-02).

Applicant—An individual requesting physical access to a facility and/or installation.

Application—A hardware and/or software system implemented to satisfy a particular set of requirements.

Architecture—A highly structured specification of an acceptable approach within a framework for solving a specific problem. Architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment and user acceptability).

Area of Influence—A geographical area wherein a commander is directly capable of influencing operations by maneuver or fire support systems normally under the commander’s command or control. (JP 1-02)

Area of Interest—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces that could jeopardize the accomplishment of the mission. Also called AOI. (JP 1-02)

Area of Operations—An operational area defined by the joint force commander for land and maritime forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called AO. (JP 1-02)

Area of Responsibility—The geographical area associated with a Combatant Command within which a geographic Combatant Commander has authority to plan and conduct operations. Also called AOR. (JP 1-02)

Authentication—A process that matches presented information to the established origin of that information.

Authenticator—A memory, possession, or quality of a person that can serve as proof of identity, when presented to a verifier of the appropriate kind. For example, passwords, cryptographic keys, and fingerprints are authenticators.

Authorization—In this publication, a process that associates permission to access a resource or asset with a person and the person’s identifier(s).

Base—A locality from which operations are projected or supported. An area or locality containing installations which provide logistic or other support. (JP 1-02).

Base Boundary—A line that delineates the surface area of a base for the purpose of facilitating coordination and deconfliction of operations between adjacent units, formations, or areas. (JP 3-10) *[The Base Boundary is not necessarily the base perimeter, rather it should be established based upon the factors of mission, enemy, terrain and weather, troops and other support available, time available (METT-T), specifically balancing the need of the base defense forces to control key terrain with their ability to accomplish the mission.]* {Italicized definition in brackets is not included in the JP 1-02 definition of Base Boundary, but found in the text of JP 3-10 as clarification of the Base Boundary}.

Base Defense—The local military measures, both normal and emergency, required to nullify or reduce the effectiveness of enemy attacks on, or sabotage of, a base, to ensure the maximum capacity of its facilities is available to US forces. (JP 1-02).

Base Defense Operations Center—A command and control facility, with responsibilities similar to a base cluster operations center, established by the base commander to serve as the focal point for base security and defense. It plans, directs, integrates, coordinates, and controls all base defense efforts. Also called BDOC. (JP 3-10). **Note:** For the purposes of this Instruction, the term “Installation Commander” is used in lieu of —Base Commander to refer to the individual responsible for defense operations performed by an installation.

Biographic Information—Facts of or relating to, a person that asserts and/or supports the establishment of their identity. The identity of U.S. citizens is asserted by their social security number and given name. Other biographic information may include, but is not limited to, identifying marks such as tattoos, birthmarks, etc.

Biometric—A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. An authenticator produced from measurable qualities of a living person.

Biometrics—A general term used to alternatively describe a characteristic or process. Stored electronic information pertaining to a biometric can be in terms of raw or compressed pixels, or in terms of some characteristics (e.g., patterns).

Biometric System—A system capable of capturing a biometric sample from a subject; extracting and processing the biometric data from that sample; storing the extracted information in a database; comparing the biometric with data contained in one or more references; matching, and indicating whether or not an identification or verification of identity has been achieved.

Capture—The method of taking a biometric sample from an end user.

Card Authentication Key (CAK)—A PIV authentication mechanism (or the PIV Card key of the same name) that is implemented by an asymmetric or symmetric key challenge/response protocol. The CAK is an optional mechanism defined in NIST SP 800-73. [SP800-73] NIST strongly recommends that every PIV Card contain an asymmetric CAK and corresponding certificate, and that agencies use the asymmetric CAK protocol, rather than a symmetric CAK protocol, whenever the CAK authentication mechanism is used with PACS.

Cardholder—An individual possessing any RAPIDS issued ID card; PIV, CAC or machine readable IDs.

Cardholder Unique Identifier (CHUID)—A FIPS 201 authentication mechanism that is implemented by transmission of the CHUID data object from the PIV Card to PACS, or the PIV Card data object of the same name.

CBRNE—Operations or incidents involving chemical, biological, radiological, nuclear, and high-yield explosives, either individually or in combination. "CBRNE" is used anytime that reference is not being made to weapon of mass destruction (WMD) operations or incidents. (AFI 10-2501)

Child—A sponsor's currently unmarried; legitimate child (born of marriage), adopted child, legitimate stepchild, or illegitimate child (see definition below). Children may receive medical benefits if they are: (1) younger than 21 years of age; (2) 21 or 22 years old and enrolled in a full-time course of education; (3) 21 or older but incapable of self-support because of a mental or physical incapacity that existed before their 21st birthday; (4) 21 or 22 years old and were enrolled full-time in an accredited institution of higher learning but became incapable of self-support because of a mental or physical condition that developed during these years. **Note:** If a sponsor provides over 50 percent support to their child, the child is also eligible for shopping privileges if they reside in the sponsor's household or maintained in a household by the sponsor.

Civilian Employee—DoD civilian employees, as defined in section 2105 of Title 5, United States Code are individuals appointed to positions by designated officials. Appointments to appropriated fund positions are either permanent or time-limited and the employees are on full-time, part-time, or intermittent work schedules. In some instances, the appointments are seasonal with either a full-time, part-time, or intermittent work schedule. Positions are categorized further as Senior Executive Service, Competitive Service, and Excepted Service positions. In addition, DoD employs individuals paid from non-appropriated funds, as well as foreign national citizens outside the United States, its territories, and its possessions, in DoD activities overseas. The terms and conditions of host-nation citizen employment are governed by controlling treaties, agreements, and memoranda of understanding with foreign nations.

Civilian Noncombatant Personnel—Personnel who have been authorized to accompany military forces of the United States in regions of conflict, combat, and contingency operations and who are liable to capture and detention by the enemy as prisoners of war (POWs).

Contactless Reader—A smart card reader that communicates with the Integrated Circuit chip in a smart card using radio frequency (RF) signaling. The PIV contactless interface is standardized by ISO/IEC 14443. [ISO/IEC14443]

Contact Reader—A smart card reader that communicates with the Integrated Circuit chip in a smart card using electrical signals on wires touching the smart card's contact pad. The PIV contact interface is standardized by International Organization of Standards / International Electrotechnical Commission (ISO/IEC) 7816-3. [ISO/IEC7816]

Control—As it relates to escorted personnel, control is defined as the ability to exercise restraint or direction of the escorted individual(s). It includes physical proximity of the sponsor except on-base residences. Sponsors do not have to be continuously present in on-base residences with their escorts to ensure control as long as the escort stays within the residence or adjoining public (uncontrolled) areas.

Controlled Area—A controlled space extending upward and outward from a specified point. Installations are generally considered controlled areas for the purposes of national defense.

FOR OFFICIAL USE ONLY

Commanders and/or directors may further designate controlled areas within an installation based upon geographic attributes and unit dispersal. Controlled areas generally designate areas wherein sensitive operations occur or controlled unclassified and sensitive information is stored and access is limited to specific persons.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called **CI**. (JP 1-02)

Credential—Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card (to include the CAC) because a CAC is a PIV) and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual. A collection of information about a person, attested to by an issuing authority. A credential may be a physical artifact (e.g., a **PIV Card**) or a data object (e.g., a **certificate**). One or more data object credentials may be stored on the same physical memory device (e.g., a smart card). **Note:** For the purposes of this instruction, credential includes CAC, Non-CAC DoD Card, Non-DoD federal PIV, TWIC, PIV-I, and locally produced PACS Passes/Cards and AF Form 75s.

Credential Validation—The process of determining if a credential is *valid*, i.e., it was legitimately issued, its activation date has been reached, it has not expired, it has not been tampered with, and it has not been terminated, suspended, or revoked by the issuing authority.

Defense Force Commander— The individual provided authority to conduct integrated defense for the senior Air Force commander responsible for an air base. The defense force commander exercises command and control through an established chain of command and directs the planning and execution of integrated defense operations. Also called **DFC**. (AFPD 31-1).

Dependent—An individual whose relationship to the sponsor leads to entitlement to benefits and privileges.

Dual Status—A person who is entitled to privileges from two sources (e.g., a retired member, who is also the dependent of an active duty member; a retired-with-pay member who is employed overseas as a civilian by the U.S. Government and is qualified for logistical support because of that civilian employment; a member of a Reserve component who is an eligible dependent of an active duty military sponsor; or a child, who is the natural child of one sponsor and the stepchild and member of a household of another sponsor).

Emergency Communications Center—The ECC is the single emergency response dispatch point and includes, as a minimum, the functions of Fire Alarm Communications Center (FACC), SF BDOC, and Medical dispatch (when applicable). The ECC has the ability to provide continuous, uninterrupted receipt and processing of emergency calls; to dispatch sufficient resources; to mitigate the emergency; to provide the required follow-on communications related to the situation; and to meet public law, national consensus standards, and AF Instructions. Also known as **ECC**. (AFI 10-2501 and ECC CONOPS).

Escorted Individuals—Personnel who require access, without determination of fitness, who must be accompanied by a sponsor with authorization to escort the individual. The escort requirement is mandated for the duration of the individual's visitation period.

Federal Information Processing Standards (FIPS)—A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Fitness—Level of character and conduct determined necessary for the basis of access control decisions.

Force Projection— The ability to project the military instrument of national power from the United States or another theater, in response to requirements for military operations. (JP 3-0)

Force Protection—Actions taken to prevent or mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities and critical information. These actions conserve the force's fighting potential so it can be applied at the decisive time and place and incorporate the coordinated and synchronized offensive and defensive measures to enable the effective employment of the joint force while degrading opportunities for the enemy. Force protection does not include actions to defeat the enemy or protect against accidents, weather or disease. (JP 1-02) [An integrated application of offensive and defensive actions that deter, detect, preempt, mitigate or negate threats against or hazards to Air Force air and space operations and assets, based on an acceptable level of risk.]{Definition in brackets applies only to the Air Force and is offered for clarity.}

Force Protection Intelligence—Analyzed, all-source intelligence information that when integrated, or fused with other FP information provides an assessment of the threats to DoD missions, people or resources. FPI is proactive and drives FP decisions in support of commander's intent.

Foreign National Civilians and Contractors—A category of personnel that, for the purposes of this instruction, are CAC-eligible if sponsored by their government as part of an official visit or assigned to work on a DoD facility and/or require access to DoD networks both on site or remotely (remote access must be on an exception only basis for this category).

Former Member—An individual who is in receipt of retired pay for non-Regular service in accordance with Chapter 1223 of Section 10147 of Title 10, United States Code, but who has been discharged from the Service and who maintains no military affiliation.

Former Spouses—Individuals who were married to a uniformed Service member for at least 20 years, and the member had at least 20 years of service creditable toward retirement, and the marriage overlapped by: 20 or more years (20/20/20); 15, but less than 20 (20/20/15); an abused spouse whose marriage overlapped by 10 or more years (10/20/10).

Full-Time Work Schedule—Full-time employment with a basic 40-hour work week.

Graduated Security—A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

Identification—The one-to-many (1:N) process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the known identity of the biometric subject whose template was matched.

Identifier (or Unique Identifier)—Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers. A data object, assigned by an authority, that unambiguously identifies a person within a defined community. For example, a Driver License number identifies a licensed driver within a State. The authority registers people and guarantees assignment of each identifier to a unique person.

Identity—The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Credential—A **credential** that contains one or more identifiers for its subject, a person. In this publication, an identity credential is designed to verify the identity of its subject through **authentication mechanisms**, either manually (see **VIS**) or electronically (see **CHUID, CAK, PKI, BIO, and BIO-A**).

Identity Management—An administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity.

Identity Management System (IdM)—Identity management system comprised of one or more systems or applications that manages the identity verification, validation and issuance process.

Identity Proofing—The process of providing or reviewing federally authorized acceptable documentation for authenticity.

Identity Registration—The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Identity Verification—The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

Information Protection—The collective policies, processes and implementation of risk management and mitigation actions instituted to prevent the compromise, loss, unauthorized access/disclosure, destruction, distortion or non-accessibility of information, regardless of physical form or characteristics, over the life cycle of the information. It includes actions to regulate access to sensitive information, controlled unclassified information and classified information produced by, entrusted to or under control of the United States Government. (Information Protection CONOPS, 1 July 2008)

Installations—A base, camp, post, station, yard, center, or other activity under the jurisdiction of the Secretary of a military department or, in the case of an activity in a foreign country, under the operational control of the Secretary of a military department or the Secretary of Defense, without regard to the duration of operational control.

Installation/Base Commander—An installation commander is the individual responsible for all operations performed by an installation. In base defense operations, the base commander is the officer assigned to command a base. (JP 1-02).

Integrated Defense—Integrated Defense is the application of active and passive defense measures, employed across the legally-defined ground dimension of the operational

environment, to mitigate potential risks and defeat adversary threats to Air Force operations. Also called **ID**. (AFPD 31-1)

Integrated Defense Council—A cross-functional governing body responsible to the Installation Commander for oversight of installation integrated Defense issues. Also called IDC. (AFPD 31-1)

Intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02)

Intergovernmental Personnel Act Employees—The Intergovernmental Personnel Act mobility program provides temporary assignment of personnel between the Federal Government and State and local governments, colleges and universities, Indian tribal governments, federally funded research and development centers, and other eligible organizations.

Intermittent Work Schedule—Employment without a regularly scheduled tour of duty.

Interoperability—For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card.

Issuer—The organization that is issuing the PIV Card to an Applicant. Typically this is an organization for which the Applicant is working.

Member—An individual who is affiliated with a Service, e.g., active duty, Reserve, active duty retired, or Retired Reserve. Members in a retired states are not former members. Please see the definition of "former member."

Multi-Factor Authentication—Authentication based on more than one factor. In some contexts, each factor is a different authenticator. In other contexts, each factor is one of "something you know, something you have, something you are" (i.e., memorized fact, token, or biometric) and thus the number of factors is 1, 2, or 3.

NACI—A personnel security investigation combining a National Agency Check and written inquiries to law enforcement agencies, former employers and supervisors, references and schools. All NACIs conducted for the DoD shall include a credit check.

Non-Appropriated Fund Positions—Non-appropriated fund employees are Federal employees within the Department who are paid from non-appropriated funds.

PACS Registration—The process of authenticating, validating, and verifying information about the PIV cardholder prior to entering the information into a PACS server. The information added during registration is then utilized to perform authentication and authorization of an individual at an access point.

Part-Time Work Schedule—Part-time employment of 16 to 32 hours a week under a schedule consisting of an equal or varied of hours per day.

Periodic Screening—The process of reviewing the background of an individual who has been determined to be eligible for physical access to installations (including additional or new checks of commercial databases, Government databases, and other information lawfully available to

security officials) at any time during the period of eligibility to determine whether that individual continues to meet the requirements for eligibility for physical access.

Permanent Employee—Career or career-conditional appointment in the Competitive or Senior Executive Service or appointment in the Excepted Service that carries no restrictions or conditions.

Personal Identification Number (PIN)—A number that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Personal Identity Verification (PIV) Card—A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personally Identifiable Information (PII)—Information that can be used to distinguish or trace an individual’s identity, such as their name, social security number, date and place of birth, mother’s maiden name, and biometric records, including any personal information which is linked or linkable to a specific individual.

Personnel Identity Management and Protection—A business process that validates, authenticates and secures an individual’s identity. The process includes: identity vetting; a binding of the identity to an identity protection and management system through the issuance of a DoD credential; the linkage of the Personal Identity Verification (PIV) credential to the individual through the use of uniquely identifying characteristics and a personal identification number; and digital authentication of the identification credential linkage to the individual.

Physical Access Control—The process of physically controlling personnel and vehicular entry to installations, facilities, and resources. Access will be either unescorted or escorted.

Physical Access Control System (PACS)—An electronic system that controls the ability of people or vehicles to enter a protected area, by means of authentication and authorization at access control points.

Physical Electronic Security System Interoperability—The ability of two or more systems or components to exchange information or electronic data and to use the information that has been exchanged.

Physical Security—That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft. (JP 1-02)

Physical Security Access Control Identity and Information Management System—A system comprised of one or more systems or applications that controls the ability of people or vehicles to enter a protected area by means of visual, manual, or electronic (or a combination of the three) authentication and authorization at entry points, and manages identity information for controlling physical access to eligible, authorized persons.

Population—The set of users for the application.

Privacy Impact Assessment (PIA)—An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii)

to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Public Key Infrastructure (PKI)—A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

Reader—A device that interfaces with a PIV Card and a Controller to execute or support execution of one or more PIV authentication mechanisms.

Reciprocal Physical Access—Mutual recognition of physical access privileges granted by an installation commander.

Registration—See “Identity Registration”.

Resources—Personnel and/or materials provided as a means of support (does not refer to monetary source for purposes of this guidance). The process of determining if an assertion is true, particularly the process of determining if a data object possesses a digital signature produced by the purported signer.

Restricted Access Area—An area (land, sea or air) in which there are special restrictive measures employed to prevent or minimize incursions and/or interference, where special security measures are employed to prevent unauthorized entry and/or movement. Restricted areas are designated and authorized by the installation and/or activity commander and/or director, properly posted, and employ multiple physical security measures.

Retired Reserve Entitled to Pay at Age 60 (Gray Area Retirees)—Reserve members who have completed 20 qualifying years for retirement and are entitled to receive pay at age 60, but have not yet reached age 60.

Revocation—The process by which an issuing authority renders an issued credential useless. For example, a Certification Authority may revoke certificates it issues. Typically, a certificate is revoked if its corresponding private key is known to be, or suspected to be, compromised, or if the certificate’s subject affiliation is changed.

Risk—Measure of consequence of peril, hazard or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).

Risk Assessment—A defined process used to fuse the procedures of analyzing threat, risks, and vulnerabilities, into a cohesive, actionable product.

Risk Management—Process and resultant risk of systematically identifying, assessing and controlling risks. Commanders/Directors are required to identify critical assets and their subsequent protection requirements, including future expenditures required for the protection requirements.

Screening—The physical process of reviewing a person’s presented biographic and other identifiable information, as appropriate, to determine their authenticity, authorization, and credential verification against a government data source through authorized and secure channels at anytime during the person’s period of physical access eligibility. This assessment identifies

derogatory actions that can be determined as disqualifying issues for current or continuing physical access eligibility standards and requirements for the resource, asset, or installation.

Seasonal Employment—Annually recurring periods of work of less than 12 months each year. Seasonal employees generally are permanent employees who are placed in non-duty and/or non-pay status and recalled to duty according to pre-established conditions of employment. Seasonal employees may have full-time, part-time, or intermittent work schedules.

Security—Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 1-02).

Security-in-Depth—A combination or layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force. Examples include the use of perimeter fences, employee and visitor entry and/or exit controls, sensors and intrusion detection systems, closed circuit video monitoring, security patrols during working and non-working hours, or other safeguards that mitigate the vulnerabilities.

Senior Executive Service Positions—Appropriated fund positions in an agency classified above General Service-15 pursuant to section 5108 or in level 4 or 5 of the Executive Schedule, or an equivalent position, which is not required to be filled by an appointment by the President by and with the advice and consent of the Senate and for which an employee performs the functions listed in Sections 311, 2102, 2103, 2105, 3132, and 5311-5318 of title 5, United States Code.

Service Project Office—The uniformed Service, National Guard and Reserve component, and agency-level office that coordinates with OUSD(P&R) on policy and functional matters related to DEERS, Real-Time Automated Personnel Identification System (RAPIDS), and Contractor Verification System (CVS) being renamed the Trusted Associate Sponsorship System, and manages identification card operations within the respective organization.

Sponsor—The person affiliated to a DoD or other Federal agency who takes responsibility for verifying and authorizing the applicant's need for an identification card.

Tactical Control—Command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to, and exercised at any level at or below the level of Combatant Command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. Also called TACON. (JP 1-02)

Temporary Assignment—An appointment for a specified period not to exceed 1 year. A temporary assignment can be extended up to a maximum of 1 additional year.

Terrorism—The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (JP 1-02)

Terrorism Threat Level—An intelligence threat assessment of the level of terrorist threat faced by US personnel and interests in a foreign country. The assessment is based on a continuous intelligence analysis of a minimum of five elements: terrorist group existence, capability, history,

FOR OFFICIAL USE ONLY

trends, and targeting. There are five threat levels: NEGLIGIBLE, LOW, MEDIUM, HIGH, and CRITICAL. Threat levels should not be confused with force protection conditions. Threat level assessments are provided to senior leaders to assist them in determining the appropriate local force protection condition. (The Department of State also makes threat assessments, which may differ from those determined by DOD.) (JP 1-02).

Threat—The perceived imminence of intended aggression by a capable entity to harm a nation, a government or its instrumentalities, such as intelligence, programs, operations, people, installations, or facilities.

Unescorted Individuals—Personnel who have been identity proofed and favorably vetted are eligible for unescorted access within the installation; but are, however, still subject to any controlled or restricted area limitations, as appropriate.

Verification—The one-to-one process of matching a biometric subject's biometric sample against his/her stored biometric file.

Verifying Official—An individual who is responsible for validating eligibility of bona fide beneficiaries to receive benefits and entitlements, and who is the only person authorized to sign block number 99 on the DD Form 1172, *Application for Uniformed Services Identification Card* 4794 *DEERS Enrollment*, or block 54 on the DD Form 1172-2, *Application for Department of Defense* 4795 *Common Access Card DEERS Enrollment*.

Vetting—An evaluation of an applicant's or a card holder's character and conduct for approval, acceptance or denial for the issuance of an access control credential for physical access.

Vulnerability—A situation or circumstance, which left unchanged, may result in the degradation, loss of life, or damage to mission-essential resources.

Ward—An unmarried person whose care and physical custody has been entrusted to the sponsor by a legal decree or other instrument that a court of law or placement agency (recognized by the Secretary of Defense) issues. This term includes foster children and children for whom a managing conservator has been designated. Wards must be dependent on the sponsor for over half of their support. An identification card issued to a ward may not reflect entitlement to medical care benefits with respect to determinations of dependency made on or after July 1, 1994 unless the child is placed in the legal custody of the member or former member as a result of an order of a court of competent jurisdiction in the United States (or a Territory or possession of the United States) for a period of at least 12 consecutive months and the child is: (1) Younger than 21 years of age; (2) Between the ages of 21 and 23 and enrolled in a full-time course of study at an institution of higher learning approved by the administering Secretary; and is, dependent on the member or former member for over one-half of the student's support or was at the time of the member's or former member's death; (3) Incapable of self support because of a mental or physical incapacity that occurred while the person was considered a dependent of the member or former member; and is, dependent on the member or former member for over one-half of the person's support or was at the time of the member's or former member's death; and, resides with the member or former member unless separated by the necessity of military service or to receive institutional care as a result of disability or incapacitation; and is, (4) Not an eligible dependent of any other member or a former member. **Note:** When documents do not appear to establish a ward relationship, refer the applicant to the base legal office.

FOR OFFICIAL USE ONLY